200307439 -- Patent Information

Publication Number	200307439
Title	**Mechanism for supporting wired and wireless methods for client and server side authentication**
Patent type	A
Date of Publication	2003/12/1
Application Number	092100518
Filing Date	2003/1/10
IPC	H04L9/32
Inventor	**KOTESHWERRAO, ADUSUMILLI**(IN)
Priority	**Country** / **Application Number** / **Priority Date**: US / 20020045893 / 2002/01/12
Applicant	**Name** / **Country** / **Individual/Company**: INTEL CORPORATION / US / Company
Abstract	Authentication functions are centralized in a security system to offload servers of this functionality, and to provide an end-to-end solution for secure internet transactions. The security system supports authentication functions for authenticating a server by requesting server certificates from a certificate authority, and sending server certificates to clients requesting authentication. The security system also authenticates clients by checking digital signatures, validating the client certificates, which includes checking CA signatures, checking the validity period of the signatures, maintaining a certificate revocation list (CRL), and checking client certificates against the CRL.

Available features

1 / 1 DWPI - The Thomson Corp. World Patents Index - ?The Thomson Corp.

2003-606507 [57] Secure client server connection establishment method involves intercepting da...

Derwent Accession	2003-606507 [57]
Cross Reference	2003-372498
Non-CPI Accession	N2003-483537
Title	Secure client server connection establishment method involves intercepting data at server on receipt of message from client, to determine whether client is authentic and accordingly establishes connection with server
Derwent Class	T01 W01
Patent Assignee	(ADUS/) ADUSUMILLI K (ITLC) INTEL CORP
Inventor	ADUSUMILLI K; KOTESHWERRAO A
Nbr of Patents	8
Nbr of Countries	99
Patent Number	US20030097592 A1 20030522 DW2003-57 H04L-009/32 Eng 43p * **AP**: 2002US-0045893 20020112, CIP of 2001US-0000154 20011023 WO200361246 A1 20030724 DW2003-58 H04L-029/06 Eng **AP**: 2003WO-US00893 20030110 AU2003214827 A1 20030730 DW2004-21 H04L-029/06 Eng **FD**: Based on WO200361246 A **AP**: 2003AU-0214827 20030110 GB2399480 A 20040915 DW2004-61 H04L-029/06 Eng **FD**: Based on WO200361246 A, Based on WO200361246 A **AP**: 2003WO-US00893 20030110, 2004GB-0015250 20040707 DE10392208 T0 20041223 DW2005-01 H04L-029/06 Ger **FD**: Based on WO200361246 A **AP**: 2003DE-1092208 20030110, 2003WO-US00893 20030110 TW200307439 A 20031201 DW2005-57 Chi **AP**: 2003TW-0100518 20030110 CN1615632 A 20050511 DW2005-58 H04L-029/06 Chi **AP**: 2003CN-0802164 20030110 GB2399480 B 20051221 DW2006-01 H04L-029/06 Eng **FD**: Based on WO200361246 A, Based on WO200361246 A **AP**: 2003WO-US00893 20030110, 2004GB-0015250 20040707
Priority Number	2002US-0045893 20020112; 2001US-0000154 20011023
Intl Patent Class	H04L-029/06; H04L-009/32; ; H04L-029/08
Advanced IPC (V8)	H04L-029/06 [2006-01 A - I R - -] H04L-029/08 [2006-01 A - I R - -]
Core IPC (V8)	H04L-029/06 [2006 C - I R - -] H04L-029/08 [2006 C - I R - -]
US Patent Class	713201000 713168000
Designated States	WO200361246 National States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW Regional States: AT BE BG CH CY CZ DE DK EA EE ES FI FR GB GH GM GR HU IE IT KE LS LU MC MW MZ NL OA PT SD SE SI SK SL SZ TR TZ UG ZM ZW

發明專利說明書 200307439

（填寫本書件時請先行詳閱申請書後之申請須知，作※記號部分請勿填寫）

※ 申請案號：92100518 ※IPC分類：H04L 9/32

※ 申請日期：92. 1. 10

壹、發明名稱

（中文）支援客戶端及伺服器端有線及無線認證方法之機構

（英文）MECHANISM FOR SUPPORTING WIRED AND WIRELESS METHODS FOR CLIENT AND SERVER SIDE AUTHENTICATION

貳、發明人（共 1 人）

發明人 1 （如發明人超過一人，請填說明書發明人續頁）

姓名：（中文）艾杜蘇彌黎 寇特斯伍羅

（英文）ADUSUMILLI KOTESHWERRAO

住居所地址：（中文）美國加州聖地牙哥市克李克橋路 10884 號

（英文）10884 CREEKBRIDGE PLACE, SAN DIEGO, CALIFORNIA 92128, U.S.A.

國籍：（中文）印度 （英文）INDIA

參、申請人（共 1 人）

申請人 1 （如申請人超過一人，請填說明書申請人續頁）

姓名或名稱：（中文）美商英特爾公司

（英文）INTEL CORPORATION

住居所或營業所地址：（中文）美國加州聖塔卡拉瓦市米遜大學路 2200 號

（英文）220 MISSION COLLEGE BOULEVARD, SANTA CLARA, CALIFORNIA 95052, U.S.A.

國籍：（中文）美國 （英文）U.S.A.

代表人：（中文）大衛 賽門

（英文）DAVID SIMON

肆、中文發明摘要

將身分鑑定功能集中於一安全系統，以便將該功能自伺服器下放，並將一種端點對端點的解決方案提供給安全互連網路交易。該安全系統支援用於鑑定一伺服器的身分之身分鑑定功能，其方式為：向一數位憑證管理機構要求伺服器憑證；以及將伺服器憑證傳送到要求身分鑑定的各用戶端裝置。該安全系統亦鑑定用戶端裝置之身分，其方式為：檢查數位簽章；確認用戶端裝置憑證，其中包括檢查數位憑證管理機構(CA)的數位簽章；檢查該等數位簽章的有效期間；維護一數位憑證廢止清冊(CRL)；以及將用戶端裝置憑證與該CRL比對。

伍、英文發明摘要

Authentication functions are centralized in a security system to offload servers of this functionality, and to provide an end-to-end solution for secure internet transactions. The security system supports authentication functions for authenticating a server by requesting server certificates from a certificate authority, and sending server certificates to clients requesting authentication. The security system also authenticates clients by checking digital signatures, validating the client certificates, which includes checking CA signatures, checking the validity period of the signatures, maintaining a certificate revocation list (CRL), and checking client certificates against the CRL.

陸、(一)、本案指定代表圖為：第 1 圖

(二)、本代表圖之元件代表符號簡單說明：

100	安全的通訊系統
110	網路存取裝置
120	公眾網路
130，130B	安全格式指示
140	安全資料
150	資料中心
160	安全系統
170	選擇系統
180	轉換系統
131	安全特性
190	埠

柒、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

捌、聲明事項

☐ 本案係符合專利法第二十條第一項☐第一款但書或☐第二款但書規定之期間，其日期為：＿＿＿＿＿＿＿＿

☑ 本案已向下列國家（地區）申請專利，申請日期及案號資料如下：

【格式請依：申請國家（地區）；申請日期；申請案號　順序註記】

1.美國；2002 年 01 月 12 日；10/045,893

2.

3.

☑ 主張專利法第二十四條第一項優先權：

【格式請依：受理國家（地區）；日期；案號　順序註記】

1.美國；2002 年 01 月 12 日；10/045,893

2.

3.

4.

5.

6.

7.

8.

9.

10.

☐ 主張專利法第二十五條之一第一項優先權：

【格式請依：申請日；申請案號　順序註記】

1.

2.

3.

☐ 主張專利法第二十六條微生物：

☐國內微生物　【格式請依：寄存機構；日期；號碼　順序註記】

1.

2.

3.

☐國外微生物　【格式請依：寄存國名；機構；日期；號碼　順序註記】

1.

2.

3.

☐熟習該項技術者易於獲得，不須寄存。

玖、發明說明

（發明說明應敘明：發明所屬之技術領域、先前技術、內容、實施方式及圖式簡單說明）

相關申請案

本申請案是2001年10月23日提出申請的待審美國專利申請案10/000, 154 "SELECTING A SECURITY FORMAT CONVERSION FOR WIRED AND WIRELESS DEVICES"之部分繼續申請案，且本申請案聲明擁有該專利申請案之優先權。

著作權通知

技術領域

本發明係大致有關網路保全能力之延伸，尤係有關一種支援用戶端數位憑證(certificate)及伺服器端數位憑證的有線及無線架構之機制。

先前技術

對安全的、可擴充的、且有使用彈性的互連網路應用及服務之需求在無線領域中正迅速地增加。當無線互連網路的應用普及時，在可處理身分鑑定及加密機制並能加速保全相關功能的裝置上有相當大的機會。

在無線互連網路領域中，無線傳輸層安全協定(WirelessTransport Layer Security；簡稱WTLS)利用加密及身分鑑定功能而提供通訊的隱私及完整性。無線通訊協定(Wireless Access Protocol；簡稱WAP)論壇的WTLS呼叫連繫協定可讓伺服器傳送其數位憑證，使伺服器向用戶端提供及本身的身分鑑定，而在用戶端與伺服器之間建立一安全連線。同樣地，如果伺服器要求用戶端的身分鑑定，則用戶端可傳送其數位憑證(或其數位憑證的一連結)而提供其本身的身分鑑定。

在有線互連網路領域中，可以安全資料傳輸層(Secure Socket Layer；簡稱SSL)的形式提供保全的功能。SSL是一種在一通訊期間支援用戶端及(或)伺服器的身分鑑定以及加密之通訊協定。

當每一代的網路變得更複雜時，有線及無線互連網路的各種應用必須是安全的。在無線互連網路技術的現行狀態下，可在WAP閘道器進行與安全相關的功能。然而，但是此種方式並未提供一種端點對端點的解決方案，這是因為使用者在WAP閘道器上被攔截，因而使用者可授權該閘道器，但不能授權伺服器。

對該問題的一解決方案以及對有線互連網路的一解決方案是將與安全相關的功能下放到這些網路中的伺服器，以便處理其中包括加密及身分鑑定的安全事務。然而，此種方式使該等伺服器剩下較少的處理效能來進行資料處理及諸如要提供給用戶端的內容之處理。

雖然某些供應商提供了在伺服器之外的與安全相關的功能，但是這些解決方案只提供了部分的安全解決方案。例如，雖然nCipher公司(位於Wobum，Massachusetts)提供了在伺服器之外的加密服務，但是並未提供身分鑑定服務。

發明內容

本發明的一個面向是一種將其中包括加密及身分鑑定的安全功能加入有線及無線互連網路的一單一網路裝置之方法，該方法將該功能及要顧慮到不同的安全標準及身分鑑定機制之需要下放到各伺服器。

該方法包含下列步驟：將一訊息自一用戶端傳送到一伺服器，以便建立一安全連線。與該伺服器相關聯的一安全系統攔截到該訊息。該安全系統執行其中包括鑑定用戶端的身分之各種身分鑑定功能、以及用於該伺服器的身分鑑定之各種支援功能。如果正確地執行了該等身分鑑定功能，則建立一安全連線。

在本文的用法中，術語互連網路(internet)包含：一網路連接(internetwork)，係將該網路連接定義為可能是不同的且係利用若干閘道器而連接在一起的一組電腦網路，而該等閘道器係處理資料傳輸以及將訊息自傳送網路的通訊協定轉換到接收網路的通訊協定；一企業內部網路(intranet)，企業內網路是一種根據諸如TCP/IP等的網際網路通訊協定但是係針對一公司或組織內的資訊管理而設計之私有網路；或網際網路(Internet)，係將網際網路

定義為使用TCP/IP通訊協定組來相互通訊的遍及全世界之一群網路及閘道器。

在下文的說明中，為了顧及解說的清晰，述及了許多特定的細節，以便可徹底了解本發明。然而，熟習此項技術者當可了解，亦可在無須某些該等特定的細節下實施本發明。在其他的情形中，係以方塊圖的形式示出習知的結構及裝置。

本發明包含將於下文中說明的各種作業。可以硬體組件來執行本發明的作業，或者可以機器可執行的指令來實施本發明的該等作業，而該等指令可用來使以該等指令來設定程式的一般用途或特殊用途處理器或邏輯電路執行該等作業。在替代實施例中，可以硬體及軟體的一組合來執行該等作業。

可以一電腦程式產品之方式提供本發明，該電腦程式產品可包含一機器可讀取的媒體，而該機器可讀取的媒體中儲存有若干指令，而可將該等指令用來設定一電腦(或其他的電子裝置)，以便執行根據本發明的一程序。該機器可讀取的媒體可包括(但不限於)軟碟、光碟、唯讀光碟(Compact Disc-Read Only Memory；簡稱CR-ROM)、磁光碟、唯讀記憶體(Read Only Memory；簡稱ROM)、隨機存取記憶體(Random Access Memory；簡稱RAM)、可抹除可程式唯讀記憶體(Erasable Programmable Read Only Memory；簡稱EPROM)、電氣可抹除可程式唯讀記憶體(Electromagnetic Erasable Programmable Read Only

Memory；簡稱EEPROM)、磁卡或光學卡、快閃記憶體、以及適於儲存電子指令的其他類型之媒體/機器可讀取的媒體。

此外，亦可將本發明下載為一電腦程式產品，其中可經由一通訊鏈路(例如一數據機或網路連線)，而利用一載波或其他傳輸媒介中包含的資料信號將該程式自一遠端電腦(例如一伺服器)傳輸到一提出要求的電腦(例如一用戶端電腦)。因此，在本文中，應將載波視為構成一機器可讀取的媒體。

實施方式

圖1示出一安全的通訊系統(100)之方塊簡圖。如本文中之說明，諸如一用來選擇一安全格式轉換的系統等的一系統可以是一包含硬體、軟體、或硬體及軟體的某一組合而用來處理資料之裝置。系統(100)包含一網路存取裝置(110)，該網路存取裝置(110)係經由一公眾網路(120)而在通訊上耦合到一資料中心(150)，以便將一安全格式指示(130)及安全資料(140)提供給資料中心(150)。該資料中心(150)包含一安全系統(160)，該安全系統(160)具有一選擇系統(170)，用以根據該指示(130)而選擇一安全轉換機制，且該安全系統(160)具有一轉換系統(180)，用以對該安全資料(140)執行所選擇的安全轉換機制。

該網路存取裝置(110)可以是可工作而連接到該網路(120)並經由該網路(120)而傳輸資料的任何電子裝置。例如，存取裝置(110)可包括一有線裝置(例如一個人電腦、

工作站)、或一無線裝置(例如一膝上型電腦、個人數位助理(Personal Digital Assistant；簡稱PDA)、行動電話、呼叫器、智慧型行動電話(smartphone)、或通訊器(communicator)。有線裝置通常使用與無線裝置不同的安全格式或通訊協定，以便利用較大的記憶體、處理器、及頻寬資源。

與可在資料中心(150)內部使用的私有網路(例如一企業內部網路)相比時，公眾網路(120)可能是較不可靠的，較不安全的，且於傳輸中更易於受到安全破壞的(例如，中間人攻擊法(man-in-the-middle attack)的入侵)。根據一實施例，公眾網路(120)包括一無線網路、一WAP閘道器、及網際網路，並在一網路存取裝置(110)與資料中心(150)之間提供端點對端點的保全。

資料中心(150)可以是與該公眾網路(120)連接的任何一個或多個電腦系統，用以經由公眾網路(120)而接收或提供安全資料。例如，資料中心(150)可包含：複數個以私有網路連接的電腦系統，用以提供諸如防火牆等的功能；一伺服器；以及一資料來源。

網路存取裝置(110)將一安全協定指示(130)經由網路(120)而傳送到資料中心(150)。可考慮該指示(130)的不同實施例。根據一第一實施例，該指示(130)包含用來要求並界定網路存取裝置(110)與資料中心(150)間的一連線之資訊。

根據一第二實施例，該指示(130)包含一埠的指示，例

如，與在組態被設定成接收一特定安全格式的一埠上接收的該特定安全格式相關聯之一訊息。術語"埠"("port")將被用來意指自網路(120)接收的資料與資料中心(150)中的諸如一應用程式、模組、或高階通訊協定等的一組件間之一邏輯連結或介面。該埠可具有一指定給該組件的對應之埠編號，且該埠編號可用來連結或指示以該組件或服務自網路(120)接收的資料。根據一實施例，該埠可包含一具有一習知埠編號的習知之埠。例如，該埠可以是用於HTTP資料的習知之埠80，或該埠可以是用於SSL資料的習知之埠443。自網路(120)接收的一訊息可包含一用來識別該組件的埠識別碼。根據一實施例，可以一接受作業系統指示的軟體程序來實施一埠，而該軟體程序係針對用來識別該埠及該組件的埠識別碼，而監視在諸如以一超高速乙太網路(gigabit Ethernet)或RJ45連線連結到網路(120)的一網路介面卡(Network Interface Card；簡稱NIC)等的一實體介面上自該網路(120)接收的資料。該埠識別碼及一IP位址合而構成用來指定一連線的一端點之一連結點(socket)。可以其中包含裝置(110)的一埠及IP位址以及資料中心(150)的一埠及IP位址之一個四元組(tuple)來指定裝置(110)與資料中心(150)間之一端點對端點通訊。

根據一第三實施例，指示(130)包含網路存取裝置(110)支援的、較適合的、或支援且較適合的一安全格式之一指示。例如，指示(130)可包含網路存取裝置(110)支援的或較適合的一安全特性，且係在諸如一安全呼叫連繫期間傳

送的用戶端招呼訊息(hello messagc)等的一資料傳輸前階段的安全協商訊息中宣告該安全特性。術語"安全特性"("security feature")將被廣泛地用來意指係描述或界定一安全格式之特性、參數、及選項，且安全特性包括(但不限於)自其中包含版本資訊、選項資訊(例如已認證或未認證)、加密演算法資訊、安全參數資訊、密碼參數資訊、可信賴數位憑證(trusted certificate)資訊、及其他安全特性資訊的一組安全特性中選出的安全特性。

根據一第四實施例，指示(130)包含與安全格式相關聯的一埠之一指示、及裝置(110)所支援的一安全特性之一指示。例如，例示指示(130B)包含提供給資料中心(150)的一埠(190)(該埠可包括習知的埠 443)之一安全特性(131)。

根據一第五實施例，指示(130)包含對應於一先前的安全格式或轉換之一交談識別碼(session identification)。根據一第六實施例，指示(130)包含可容許使用來自資料中心(150)中的一使用者定義檔(profile)的一安全格式或安全轉換機制之一使用者定義檔識別碼(profile identification)(例如一使用者識別碼及密碼)。根據一第七實施例，指示(130)包含諸如SSL 3.0版等的一安全格式的一專用之明確識別碼。根據一第八實施例，指示(130)包含諸如自SSL 3.0版轉換為平常資料的一邏輯單元或一模組等的一安全轉換機制的一專用之明確識別碼。亦可考慮使用指示(130)的許多其他實施例，且對此項技術具有一

般程度知識者在參閱本發明揭示事項之後將可了解：應廣義地詮釋該指示(130)。

如前文所述，可考慮使用不同的指示(130)，且選擇系統(170)可因而作出不同的選擇。根據一第一實施例，該選擇係根據自網路(120)接收的資訊。根據一第二實施例，該選擇係根據與在網路存取裝置(110)與資料中心(150)之間建立一連線相關聯之連線資訊。根據一第三實施例，該選擇係根據埠資訊。例如，如果是在一第一預定的經組態設定之埠上接收連線資訊，則選擇系統(170)可選擇一第一轉換機制；而如果是在一第二埠上接收接收連線資訊，則選擇系統(170)可選擇一第二轉換機制。根據一第四實施例，該選擇係根據用來指示裝置(110)支援的、較適合的、或支援且較適合的安全格式之安全特性資訊。例如，選擇系統(170)可根據在一用戶端招呼訊息中宣告的一支援且較適合的安全格式而選擇一轉換機制。

根據一第五實施例，該選擇可根據埠資訊及安全特性資訊。例如，選擇系統(170)可根據用來接收一用戶端招呼訊息的一埠、以及該用戶端招呼訊息中指示的用戶端裝置(110)支援且較適合的安全特性，而選擇自一安全格式的轉換機制。

根據一第六實施例，該選擇可根據對應於一先前的安全格式或轉換機制之一交談識別碼。根據一第七實施例，該選擇可根據可讓選擇系統(170)使用來自一使用者定義檔的一安全格式或安全格式轉換機制之一使用者定義檔識

別碼。根據一第八實施例，該選擇可根據所陳述的一安全格式或安全格式轉換機制(例如，"自SSL V 3.0版本轉換為平常資料")。亦可考慮使用許多其他的選擇及選擇系統(170)，且對此項技術具有一般程度知識者在參閱本發明揭示事項之後將可了解：應廣義地詮釋該選擇及該選擇系統(170)。

該轉換係自所接收的安全格式轉換為另一格式。該另一格式可以是一平常未加密的資料格式。當資料中心(150)具有足夠的內部安全性，且對非故意地或未經授權地存取資料有足夠低的風險時，上述的轉換可能是有利的。此種方式的有利之處在於可避免資料中心(150)內的一後續之解密。根據一替代實施例，該另一格式可以是一不同的安全格式。亦即，安全系統(160)可選擇並執行自一安全格式轉換為一不同的安全格式。例如，該轉換可以是轉換為IP安全(IPSec)，而資料中心(150)的一企業內部網路內的保全可能需要此種安全格式。

網路存取裝置(110)將安全資料(140)經由網路(120)而傳送到資料中心(150)。資料中心(150)自網路(120)接收該安全資料(140)。轉換系統(180)對該安全資料(140)執行所選擇的安全格式轉換。在未加限制下，該安全資料(140)可以是交易資料及(或)金融資料，且資料中心(150)可視特定實施例的需要而使用及(或)回應該資料。

根據一實施例，該網路存取裝置(110)是一使用圖2所示的一WAP堆疊(200)與資料中心(150)通訊之一無線網路存

取裝置。WAP堆疊(200)是一安全規格，可讓無線裝置經由網路(120)而存取資訊。WAP堆疊(200)包含一應用層(210)、一交談層(220)、一交易層(230)、一安全層(240)、一傳輸層(250)、及一網路層(260)。WAP堆疊(200)是對此項技術具有一般知識者所習知的，且係詳述於WAP規格的1.2版及2.0版，可自網站http://www.wapforum.org取得該規格。

安全層(240)包含WTLS通訊協定，且可將隱私、資料完整性、及用戶端/伺服器身分鑑定提供給WAP起動的無線裝置。WTLS通訊協定係在傳輸層(250)之上作業，並將一安全傳輸服務介面提供給該等較上層的WAP層(210-230)，該介面保留了下層的傳輸介面，也提供了用來管理安全連線的方法。WTLS係與諸如安全資料傳輸層(SSL)等的非無線通訊協定有關，但涉及較低裝置端的處理能力及記憶體要求、較低的頻寬、以及資料元(datagram)連接。

傳輸層(250)可包含諸如UDP/IP及WDP等不同的資料元型傳輸層通訊協定。UDP係配合IP載送服務(bearer service)而作業，而WDP係配合非IP載送服務而作業。例如，可配合簡訊服務(Short Message Service；簡稱SMS)及類似的無線載送服務而使用WDP，而可配合電路交換資料(Circuit Switched Data；簡稱CSD)及類似的載送服務而使用UDP。

圖3示出本發明一實施例的系統架構(300)之一方塊簡圖。系統架構(300)包含一無線存取裝置(305)及一有線存

取裝置(320)，用以不同方式加密的訊息經由一公眾網路(325)而傳送到一資料中心(340)，該資料中心(340)包含一安全系統(345)，用以選擇並執行對所接收的以不同方式加密之訊息之不同的安全格式轉換處理。

無線存取裝置(305)在一實施例中是一可使用WAP微型瀏覽器之細胞式電話，該無線存取裝置(305)係經由一無線網路(310)及WAP閘道器(315)而耦合到公眾網路(325)(在一實施例中為網際網路)。無線存取裝置(305)產生一包含對應於裝置(305)的安全能力及偏好的安全特性資訊之WTLS用戶端招呼訊息，並利用UDP或WDP傳輸協定而將該WTLS用戶端招呼訊息傳送到無線網路(310)。無線網路(310)接收該訊息，並將該訊息傳送到該WAP閘道器。該WAP閘道器將該傳輸協定媒體自UDP或WDP轉換為TCP，然後利用TCP將該訊息傳送到公眾網路(325)。

根據一實施例，該有線存取裝置(320)是一可使用瀏覽器的個人電腦，該有線存取裝置(320)產生一包含安全特性資訊之訊息，並將該訊息傳送到公眾網路(325)。該訊息可包含用來開始在一SSL呼叫連繫中協商一安全格式之一SSL用戶端招呼訊息。

公眾網路(325)係在功能上連接到無線存取裝置(305)、有線存取裝置(320)、及資料中心(340)，以便自該等裝置(305)、(320)接收該等訊息，並將該等訊息提供給資料中心(340)。根據一實施例，網路(325)包括網際網路，且可使用TCP或UDP作為傳輸媒體之通訊協定。網路(325)將該

等訊息傳輸或傳送到資料中心(340)，作為指示(330)及(335)。

資料中心(340)係耦合到公眾網路(325)，以便接收與該等裝置(305)及(320)相關聯的訊息。資料中心(340)包含一安全系統(345)，而根據一實施例，該安全系統(345)係在功能上配置於公眾網路(325)與一伺服器(390)之間，因而安全系統(345)可執行安全格式轉換之選擇，並代表伺服器(390)而執行作業。

根據一實施例，安全系統(345)包含：一網路介面(350)，用以接收指示及安全資料；一選擇系統(360)，用以根據該等指示而選擇一轉換；一轉換系統(370)，用以接收所選擇的轉換，並對經由網路介面(350)而接收的安全資料執行所選擇的轉換；以及一第二網路介面(380)，用以接收轉換後的資料，並將該轉換後的資料提供給其他的資料中心(340)組件，例如在一實施例中係將該資料提供給一伺服器(390)。

網路介面(350)可包括一個或多個NIC，用以代表資料中心(340)接收該等訊息及安全資料。根據一實施例，網路介面(350)包含用來自無線存取裝置(305)接收資訊的至少一個埠(354)、以及用來自有線存取裝置(320)接收資訊的至少一個埠(352)。例如，網路介面(350)可包含：一第一及第二埠(354)，用以分別自無線存取裝置(305)接收安全的及不安全的資料；以及一第二及第三埠(352)，用以分別自有線存取裝置(320)接收安全的及不安全的資料。

選擇系統(360)係耦合到網路介面(350)，以便自網路介面(350)接收安全格式轉換選擇資訊，並根據該資訊而選擇一安全格式轉換。該安全格式轉換可以是自與該資訊相關聯的一安全格式轉換為另一種格式(例如另一種安全格式或一平常資料格式)。根據一第一實施例，選擇系統(360)係根據所接收的一埠之指示而選擇一安全格式轉換。例如，選擇系統(360)可能接收習知係用於SSL加密資料的一預定埠之一指示，並選擇自SSL加密格式轉換為另一格式的至少一種安全格式轉換。根據一第二實施例，選擇系統(360)係根據所接收的安全特性資訊而選擇至少一種安全格式轉換。例如，選擇系統(360)可接收用來指示有線存取裝置(320)支援的一安全特性或一組安全特性之安全特性資訊，並選擇自該安全特性轉換為另一格式之一轉換。根據一第三實施例，選擇系統(360)係根據埠資訊及安全特性資訊而選擇一轉換。例如，選擇系統(360)可根據埠資訊而選擇一具有自一WTLS格式轉換為另一格式的至少一個特定轉換之WTLS轉換系統(372)、或一具有自一SSL格式轉換為另一格式的至少一個特定轉換之SSL轉換系統(374)，並可根據安全特性資訊而選擇該特定的WTLS或SSL轉換。

選擇系統(360)可將所選擇的安全格式轉換提供給其他的系統(300)組件。根據一實施例，選擇系統(360)使一裝置(305)或(320)與資料中心(340)間之一交談的一交談識別碼與該所選擇的安全格式轉換相關聯。此種方式可讓後

續接收到的安全格式之資料與該所選擇的安全格式轉換相關聯。在一實施例中，選擇系統(360)可觸發一安全格式轉換選擇信號，而將所選擇的轉換通知轉換系統(370)。例如，選擇系統(360)可對載送所選擇的該轉換之轉換系統(370)、WTLS轉換系統(372)、或SSL轉換系統(374)進行一方法呼叫。

在裝置(305)、(320)與安全系統(345)之間已協商出一個安全格式之後，裝置(305)、(320)可將安全資料傳送到安全系統(345)。更具體而言，無線裝置(305)可在一預定版本的WTLS中傳送資料。無線網路(310)可接收該安全資料，並將該安全資料提供給WAP閘道器(315)。WAP閘道器(315)通常將執行自UDP或WDP轉換為TCP，並將TCP格式的資料提供給公眾網路(325)。

根據一實施例，WAP閘道器(315)之組態被設定成讓所接收的WTLS安全資料通過，而無須進行安全格式轉換。此種方式的有利之處在於可在無線存取裝置(305)與資料中心(340)之間提供端點對端點的安全防護，且可消除當經由一對中間人攻擊法開放的一易被侵入的平常資料狀態而將WTLS資料轉換為SSL資料時存在的WAP缺口。可考慮使用不同的組態設定，而該等組態設定包括將WAP閘道器(315)之組態被設定成讓所有到資料中心(340)的無線連接信號通過而無須進行安全格式轉換之組態設定。與圖1-3所示之先前技術方式比較時，此種方式也提供了較短的延遲時間，這是因為可免掉不必要的安全格式轉

換處理及傳輸進出系統(300)所需之時間。

有線存取裝置(320)可在已與安全系統(345)協商出的一預定版本之SSL中傳輸資料。可使用網際網路(325)上的TCP而以SSL格式傳輸該資料。

轉換系統(370)係耦合到選擇系統(360)，以便接收所選擇的安全格式轉換，且轉換系統(370)係耦合到網路介面(350)，以便自無線裝置(305)及有線裝置(320)接收安全資料。轉換系統(370)對所接收的安全資料執行所選擇的轉換。轉換系統(370)可包含其中包括軟體、硬體、或軟體及硬體之某一組合之邏輯單元，用以將所接收的安全資料(例如WTLS或SSL加密資料)解密成一平常未加密的資料，且如有需要，則可再重新加密成一替代性的安全協定格式。根據一實施例，該邏輯單元可包含對此項技術具有一般知識且參閱過本發明的揭示事項之人士所習知的傳統之轉換邏輯單元。

如前文所述，安全系統(345)可包含不同的轉換模組，用以執行將一接收的安全格式轉換為另一格式。根據一實施例，轉換系統(370)包含一WTLS轉換系統(372)及一SSL轉換系統(374)，用以將WTLS或SSL安全資料分別轉換為一不同的安全格式。WTLS轉換系統(372)可包含複數個轉換模組，例如，可包含將具有一第一安全特性的一第一版本的WTLS轉換為平常資料之一第一轉換模組、將具有一第二安全特性的一第二版本的WTLS轉換為平常資料之一第二轉換模組、以及將該第一版本的WTLS轉換為諸如

SSL、IPSec、或其他格式等的另一安全格式之一第三轉換模組。同樣地，轉換系統(374)可具有複數個轉換模組。

轉換系統(370)將轉換後的資料提供給一耦合到伺服器(390)之網路介面(380)。該網路介面(380)可包括一NIC。網路介面(380)通常係將平常資料經由諸如埠80等的一平常資料埠而提供給伺服器(390)，但是亦可考慮採用其他的實施例。

伺服器(390)接收轉換後的資料。如果轉換後的資料是一安全格式，則伺服器(390)可執行解密。伺服器(390)可不受限制而執行特定實施例所需的任何處理。該處理供常包括將回應資料經由安全系統(345)而提供給裝置(305)、(320)。根據一實施例，伺服器(390)將平常資料提供給安全系統(345)。

安全系統(345)可接收該回應資料，並對該資料執行安全處理。根據一實施例，安全系統(345)係以一種大致與原始轉換相反之方式處理該回應資料。例如，對於無線裝置(305)的回應資料而言，安全系統(345)可將來自伺服器(390)的平常資料轉換為WTLS格式，並將該安全資料提供給無線裝置(305)。同樣地，對於有線裝置(320)的回應資料而言，安全系統(345)可將來自伺服器(390)的平常資料轉換為SSL格式，並將該安全資料提供給有線裝置(320)。

系統(300)可提供若干優點。第一個優點可以是能夠將安全處理功能自伺服器(390)下放到安全系統(345)。安全

處理可能是一種處理器及記憶體使用率相當高的工作，且在未將負載下放的情形下，可能耗用相當多的伺服器(390)資源。負載下放亦可使伺服器(390)處理更多的連線。例如，以一安全系統(345)執行安全格式轉換時，伺服器(390)可處理的連線數目是未設有該安全系統時的大約5-10倍。

第二個優點是存取裝置(305)、(320)與伺服器(390)間之端點對端點安全防護。第三個優點是存取裝置(305)、(320)與伺服器(390)間之一單一的安全格式轉換。此種方式因具有較少的計算及較短的延遲，而提供了較快速的資料交換。第四個優點是安全系統(345)可將一單一點的安全防護解決方案提供給無線及有線安全協定。第五個優點是：與伺服器(390)的更新相比時，以最新的安全標準及格式轉換來更新安全系統(345)經常是較為容易的。

已以簡化的形式示出了安全系統(345)，以便不會模糊了本發明。然而，對此項技術具有一般知識且已參閱本發明揭示事項的人士將可了解，可在安全系統(345)中包含其他的組件(385)。該等其他的組件(385)經常將包括一作業系統或平台。該等其他的組件(385)亦可包括特定實施例可能需要的組件，例如，用來執行XML變換、XML剖析(parsing)、基於內容的路徑決定、及其他平常資料的功能。該等其他的組件(385)可包括用於諸如分別由Intel Corporation(位於Santa Clara, California)所供應的Intel(R) NetStructure TM 7110 e-Commerce Accelerator、7115 e-Commerce Accelerator、7140 Traffic Director

、7175 Traffic Director、7180 e-Commerce Director、7280 XML Director、或7210 XML Accelerator等的傳統專用安全防護加速器之組件。

圖4以方塊圖示出根據一實施例而操作諸如安全系統(160)或(345)等的一安全系統之一方法(400)。可以可包括軟體、硬體、或軟體及硬體的一組合之邏輯單元來實施該方法(400)。

方法(400)開始於步驟(401)，然後繼續進入步驟(405)，此時設定該安全系統之組態。根據一實施例，該步驟可包括讀取一其中包含系統組態設定資訊的組態設定檔。例如，該安全系統可在不受限制的情形下存取諸如下表中包含的組態設定資訊：

表1

連線圖識別碼	連線類型	密鑰識別碼	伺服器IP	網路埠	伺服器埠	密碼套件	重新導向
1	WTLS	WAPSRV	10.1.1.30	9208	80	低	有
2	SSL	HTTPSRV	10.1.1.31	443	80	中等	有
3	HTTP/PLAIN	無	10.1.1.31	80	80	無	無
4	WAP/PLAIN	無	10.1.1.30	80	80	無	無

在上表中，連線圖識別碼提供一連線的一任意識別碼，連線類型提供安全的或不安全的一連線類型，密鑰識別碼提供安全連線所使用的密鑰識別碼，伺服器IP用來與資料中心中的各伺服器通訊之一網際網路通訊協定位址，網路埠提供用來自一公眾網路接收安全的或不安全的資料之

預定的習知埠編號，伺服器埠提供用來將平常資料傳送到資料中心中的該等伺服器之一習知的預定埠，密碼套件包含安全及不安全的連線所用的安全防護強度之一指示，且重新導向在一存取裝置不支援所使用的安全特性時提供將一存取裝置重新導向到安全升級資源之一選項。

在不受限制的情形下考慮下文所述的重新導向功能的實施例。該安全系統決定用戶端裝置是否符合組態設定檔中指定的安全等級。如果用戶端裝置不符合所指定的安全等級，則該安全系統可決定是否要以一通用資源位標(Uniform Resource Locator；簡稱URL)的形式來傳送一重新導向網頁，以便提供該用戶端裝置升級到所指定的安全等級之機會。如果並未傳送該重新導向網頁，則可替代性地傳送一系統預設的錯誤訊息。

在替代實施例中，並不使用若干不同的伺服器，而是可將相同的伺服器用來服務不同網路埠上的HTML及無線標記語言(Wireless Markup Language；簡稱WML)內容，因而該伺服器IP及網路埠的組合是唯一的。例如，該安全系統可使用諸如下表中包含的組態設定資訊：

表 2

連線圖識別碼	連線類型	密鑰識別碼	伺服器IP	網路埠	伺服器埠	密碼套件	重新導向
1	WTLS	WEBSRV1	10.1.1.32	9208	80	低	有
2	SSL	WEBSRV2	10.1.1.32	443	80	中等	有
3	PLAIN	無	10.1.1.32	80	80	無	無

該方法(400)自步驟(405)進入步驟(410)，此時各程序監視各組態被設定的埠之活動或訊息。根據一實施例，該等程序監視由一IP位址及一埠的一唯一組合構成之若干唯一的連結點(socket)。根據一實施例，該安全系統產生若干獨立的程序或執行緒來監視組態設定檔中所識別的該等埠。例如，一程序可監視埠9203上的與WTLS相關之訊息，一程序可監視埠443上的與SSL相關之訊息，以及一程序可監視埠80上的不安全之資料。

如果在埠9208上接收到安全特性資訊，則方法(400)可自步驟(410)進入步驟(415)。根據一實施例，該安全特性資訊可包含來自一無線存取裝置之一用戶端招呼訊息。例如，該安全特性資訊可包含一現有或未來版本的WTLS之一用戶端招呼訊息。

方法(400)自步驟(415)進入步驟(420)，此時協商一WLTS安全格式。該協商可根據用來指示該無線裝置較適宜使用的或可使用的各安全特性之安全特性資訊。該協商可包括相互交換安全特性能力及(或)該存取裝置及該資料中心對同意一相互支援的安全格式之偏好。根據一實施例，步驟(420)的該協商包括一WTLS呼叫連繫協定。亦可考慮使用所協商的安全格式之不同實施例。根據一第一實施例，該安全格式包括一現有或未來版本的WTLS。根據一第二實施例，該安全格式包括諸如一加密參數、一加密演算法(例如資料加密標準(Data Encryption Standard；簡稱DES))、或以上兩者等的一協商之安全特性。

方法(400)自步驟(420)進入步驟(425)，此時選擇自所協商的該安全格式轉換為一未加密的平常資料格式之一轉換。在以一充分受信賴的連線或網路將該安全系統耦合到一資料目的地(例如資料中心伺服器)之架構中，轉換為平常資料格式可能是有利的，這是因為該伺服器可隨即接收平常資料，而無須執行解密。

根據一第一實施例，係根據埠9208上的資訊之接收情形而選擇該轉換。例如，可根據與步驟(415)相關聯的資訊而選擇該轉換。根據一第二實施例，該轉換係根據一安全協商。例如，可根據與步驟(420)相關聯的資訊而選擇該轉換。可將所選擇的安全格式轉換傳送到諸如一轉換系統或一轉換模組等其他的組件。

方法(400)自步驟(425)進入步驟(430)，此時接收到經過安全加密的資料。可經由埠9208而接收安全資料，且該安全資料可能是在步驟(420)的協商出來之安全格式中。方法(400)自步驟(430)進入步驟(435)，此時將所接收的加密資料轉換為平常資料。可利用傳統的或習知的方法來執行上述步驟。可使用一批次模式或連續模式來執行步驟(430)及(435)。

如果係在埠443上接收到安全特性資訊，則方法(400)可自步驟(410)進入步驟(440)。例如，該安全特性資訊可能與用來指示該用戶端裝置將嘗試連接到埠443的資料中心之一連線https://www.intel.com相關聯。根據一實施例，該安全特性資訊可包括來自一無線存取裝置之一用戶端

招呼訊息。例如，該安全特性資訊可包括一現有或未來版本的SSL之一用戶端招呼訊息。

方法(400)自步驟(440)進入步驟(445)，此時協商一SSL安全格式。可以一種與前文中參照步驟(420)所述的方式類是之方式來執行該協商，以便決定可基於SSL的一種安全格式，且該安全格式可包括SSL加密參數及SSL演算法。

方法(400)自步驟(445)進入步驟(450)，此時選擇自所協商的安全格式轉換為一未加密的平常資料格式之一轉換。根據一第一實施例，係根據埠443上的資訊之接收情形而選擇該轉換。例如，可根據與步驟(440)相關聯的資訊而選擇該轉換。根據一第二實施例，該轉換係根據一安全協商。例如，可根據與步驟(445)相關聯的資訊而選擇該轉換。

方法(400)自步驟(450)進入步驟(455)，此時在埠443上接收所協商的安全格式中之資料。方法(400)自步驟(455)進入步驟(460)，此時將所接收的資料自該安全格式轉換為一平常資料格式。

如果在埠80上接收到未加密的平常資料，則方法(400)可自步驟(410)進入步驟(465)。

方法(400)可自步驟(435)、(460)、或(465)進入步驟(470)，此時將平常資料提供給一所需之目的地。根據一實施例，係將該資料提供給該資料中心的一伺服器或其他的電腦系統。可以組態設定資訊中之一網址來識別該伺服器。根據一實施例，可將該資料經由習知的埠80而提供給該伺服

器。該方法(400)可終止於步驟(475)。

亦可考慮使用方法(400)的替代實施例。根據一第一替代實施例，係設定不同埠的組態，並使用該等不同埠。用來接收安全特性資訊及資料的該等埠通常將符合網際網路數字配置機構(Internet Assigned Number Authority；簡稱IANA)或一類似機構所提供之命名。根據一實施例，該WTLS埠可以是自具有在9208與9282間的數字的一組埠中選出的一埠。根據一第二替代實施例，可選擇自步驟(420)或(445)的該協商出之格式轉換為不同於一平常資料格式的另一安全格式之一安全格式轉換。當以一並非充分安全的鏈路將該資料目的地耦合到該安全系統時，上述的安全格式轉換方式可能是有利的。例如，並不提供步驟(470)中之平常資料，而是可將WTLS格式的安全資料轉換為SSL格式的安全資料；並將轉換後的安全資料提供給該資料目的地。當該資料目的地無法將先前轉換的安全格式解密時，上述的此種轉換可能是有利的。

圖5示出根據一實施例的WTLS安全架構(500)。該架構(500)包含一記錄協定(550)，該記錄協定(550)係用來：自各上堆疊層接受將要被傳輸的不安全的資料，處理資料完整性，並將壓縮及加密演算法應用於該資料。架構(500)亦包含四個用戶端協定，其中包括將於下文中說明的一呼叫連繫協定(510)、提供將安全連線終止的方式之一警示協定(520)、作為各上堆疊層的介面之一應用協定(530)、以及可在讀取、寫入、與待處理狀態之間進行協調後的改

變之一改變密碼規格協定(540)。

該呼叫連繫協定(510)代表一無線存取裝置與一資料中心間之一安全協商的一實施例。呼叫連繫協定(510)可讓該裝置與該資料中心協商或同意安全方法以及諸如安全協定、協定版本、加密演算法、身分鑑定、公開金鑰(public key)技術、及其他安全特性等的參數。

圖6示出根據一實施例的一WTLS呼叫連繫(600)之一方塊流程圖。可將該呼叫連繫(600)用來在一無線存取用戶端裝置(610)與一資料中心伺服器(670)之間協商一安全格式。根據一實施例，該呼叫連繫(600)包含安全特性資訊。

該呼叫連繫(600)開始時係由用戶端裝置(610)在步驟(620)中將一用戶端招呼訊息提供給一資料中心(670)。該用戶端招呼訊息通常宣告所支援的安全特性(例如協定、版本、選項、加密演算法、及可信賴數位憑證)。根據一實施例，該用戶端招呼訊息至少部分指示一安全格式。在該用戶端招呼訊息之後，無線存取用戶端裝置(610)接收訊息，直到資料中心伺服器(670)傳送一伺服器招呼已執行訊息為止。

呼叫連繫(600)自步驟(620)進入步驟(630)，此時資料中心伺服器(670)繼續呼叫連繫(600)。資料中心伺服器(670)可提供用來同意或重新協商安全格式方法及參數之一伺服器招呼訊息。伺服器(670)亦可傳送：一伺服器數位憑證訊息(在要使用身分鑑定的情形下)；一伺服器金鑰交換

訊息，用以提供一可用來進行或交換一主秘前值(pre-master secret value)之一公開金鑰；一數位憑證要求訊息，用以向用戶端裝置要求一數位憑證及身分鑑定；以及一伺服器招呼已執行訊息，用以指示以完成該呼叫連繫(600)之招呼訊息階段。伺服器(670)然後等候來自用戶端裝置(610)的一回應。

呼叫連繫(600)自步驟(630)進入步驟(640)，此時存取用戶端裝置(610)繼續呼叫連繫(600)。用戶端裝置(610)可傳送：一用戶端裝置數位憑證訊息(在向其要求身分鑑定的情形下，或遇到無數位憑證警示的情形下)；根據自用戶端招呼訊息及伺服器招呼訊息中選出的公開金鑰演算法之一用戶端裝置金鑰交換訊息，且該訊息包含一以該資料中心伺服器的公開金鑰加密之主秘前值；一數位簽章證書證實訊息，用以在用戶端裝置(610)已傳送一具有簽章能力的數位憑證時，明確地證實該數位憑證；一改變密碼規格訊息，用以指示利用所協商的安全參數而開始進行；以及一包含先前資料的確認之完成訊息，而該先前資料包括在新的演算法下計算出的安全資訊、金鑰、及主秘值。

呼叫連繫(600)自步驟(640)進入步驟(650)，此時資料中心伺服器(670)繼續呼叫連繫(600)。資料中心伺服器(670)可以下列訊息作為回應：一密碼規格訊息，用以確認該交談，並通知用戶端裝置(610)使用所協商的該等交談參數；以及一完成訊息，該完成訊息包含所交換的及計算的資訊之確認。

呼叫連繫(600)自步驟(650)進入步驟(660)，此時用戶端裝置(610)及伺服器(670)可利用所建立及協商的安全連線交換安全資料。呼叫連繫(600)亦可包括保留諸如交談識別碼等與該安全連線有關的資訊，以便未來的安全資料交換可根據先前協商出來的安全方法及參數。

圖7示出根據一實施例的一用戶端招呼訊息(700)。該用戶端招呼訊息(700)可用於SSL、WTLS、或其他的安全格式。根據一實施例，在一埠上接收的用戶端招呼訊息(700)包含一安全格式的指示。用戶端招呼訊息(700)包含諸如用戶端裝置安全能力資訊(710)、隨機結構資訊(720)、交談識別碼資訊(730)、支援的密碼選項資訊(740)、及壓縮方法資訊(750)等的安全特性資訊。

用戶端裝置安全能力資訊(710)可包括一協定版本。該協定版本可以是該用戶端裝置可使用的、想要使用的、或同時合乎以上兩者的一版本。例如，資訊(710)可指示SSL V 3.0版、或另一協定版本。根據一實施例，一資料中心中之一安全系統可將該用戶端裝置版本資訊用來協商一安全格式並選擇一對應的安全格式轉換。

隨機結構資訊(720)可包括一用戶端裝置產升的隨機結構。該隨機結構可包含：根據以該用戶端裝置的內部時鐘為依據的現在時間及日期之複數個位元、以及由一安全隨機數產生器產生的複數個隨機位元組。

交談識別碼資訊(730)可包括一可變長度之交談識別碼，該交談識別碼如果不是空的時，將識別該用戶端裝置與

該伺服器間之一先前的交談，而該先前的交談包括該用戶端裝置希望在現行交談中重新使用的先前之安全方法及參數。該交談識別碼可能來自於一先前的連線、現行連線、或另一目前使用中的連線。該伺服器可界定該交談識別碼的實際內容。如果無法使用一先前的交談，或者如果該用戶端裝置希望重新協商安全方法及參數，則該交談識別碼資訊(730)可以是空的。根據一實施例，一交談識別碼包含一安全格式轉換的一指示。例如，一交談識別碼可對應於一先前選擇的安全格式轉換，且接收到該交談識別碼時，可讓一選擇系統重新選擇安全格式轉換。

支援的密碼選項資訊(740)可包括該用戶端裝置所支援的且係根據該用戶端裝置的偏好而安排的各密碼選項及組合之一指示。該資訊亦可包括來自將要重新使用的先前交談之類似資訊。

壓縮方法資訊(750)可包括該用戶端裝置所支援的壓縮演算法或方法之一清單、以及用戶端裝置對每一種方法的偏好之一指示。如果交談識別碼資訊(730)指示要重新使用一交談，則壓縮方法資訊(750)可包括先前交談所使用的一壓縮方法。根據一實施例，該資訊(750)指示對CompressionMethod.null的支援。

圖8示出一實施例的一選擇系統(800)。選擇系統(800)接收一指示(810)。該指示(810)是一足以讓選擇系統(800)選擇一安全格式轉換的指示。所示之該指示(810)包括一安全格式的一指示，且具有埠資訊(812)及安全特性資訊

(814)。

將可包括用來接收資料(例如用戶端招呼訊息、安全特性資訊等的資料)的一埠之一指示之埠資訊(812)提供給選擇系統(800)的協定選擇邏輯(820)。協定選擇邏輯(820)可工作而根據埠資訊(812)在各不同的安全協定中作出選擇。根據所示之實施例，協定選擇邏輯單元(820)可工作而根據埠資訊(812)在一無線協定、一有線協定、及一平常不安全的協定中作出選擇。在不受限制下考慮下列的概念性協定選擇邏輯(820)：如果埠資訊(812)指示埠9208，則選擇一無線協定；否則，如果埠資訊(812)指示埠443，則選擇一有線協定；否則，如果埠資訊(812)指示埠80，則選擇一平常不安全的協定。協定選擇邏輯(820)觸發一協定選擇(830)，用以指示無線協定(無線選擇)、有線協定(有線選擇)、或平常不安全的協定。

選擇系統(800)亦包含與協定選擇邏輯(820)耦合之安全特性選擇邏輯(840)，用以接收協定選擇(830)。該邏輯(840)可工作而根據協定選擇(830)及安全特性資訊(814)選擇不同的安全格式轉換。選擇S5可繞過邏輯(840)，這是因為通常將不會對平常資料執行一安全格式轉換。根據所示之實施例，邏輯(840)可工作而在四個不同的轉換(亦即對應於選擇S1、S2、S3、或S4)中選擇一個轉換，但這不是對其他實施例的一限制。

邏輯(840)包含一無線邏輯部分(850)及一有線邏輯部分(860)，這兩個部分都可接收該安全特性資訊(814)。如果

協定選擇(830)指示一無線選擇，則邏輯部分(850)可工作而選擇一轉換。在不受限制下考慮下列概念性的邏輯部分(850)：如果安全特性資訊(814)指示一組F1的至少一個安全特性，則選擇一第一安全格式轉換；否則，如果安全特性資訊(814)指示一組F2的至少一個安全特性，則選擇一第二安全格式轉換；否則，如果在有將組態設定成傳送一重新導向URL的情形下，傳送一重新導向URL。

如果協定選擇(830)指示一有線選擇，則邏輯部分(860)可工作而選擇一轉換。在不受限制下考慮下列概念性的邏輯部分(860)：如果安全特性資訊(814)指示一組F3的至少一個安全特性，則選擇一第三安全格式轉換；否則，如果安全特性資訊(814)指示一組F4的至少一個安全特性，則選擇一第四安全格式轉換；否則，如果在有將組態設定成傳送一重新導向URL的情形下，傳送一重新導向URL。

邏輯(840)觸發一安全格式轉換選擇(870)，用以指示要對與埠資訊(812)及(814)一致的安全資料執行的一安全格式轉換。選擇(870)可包括用於一無線裝置的S1或S2、以及用於一有線裝置的S3或S4。可將該選擇(870)傳送到一轉換系統或模組。

圖9示出根據一實施例的一資料中心(900)。可將資料中心(900)耦合到諸如網際網路等的一公眾網路，以便自該公眾網路接收指示及安全資料。資料中心(900)包含一安全系統(920)，該安全系統(920)係在功能上配置於一交換器/路由器(910)與一交換器/路由器(930)之間，且充分地

接近資料中心(900)的一個或多個伺服器(940-960)。安全系統(920)自交換器/路由器(910)接收可能以不同的方式加密之資料，並將經過適當安全格式轉換過的資料提供給交換器/路由器(930)。交換器/路由器(930)將可能是平常資料格式的轉換後資料提供給一個或多個伺服器(940-960)。根據一第一實施例，該等一個或多個伺服器(940-960)包括：一WML內容伺服器(940)，可以一網址10.1.1.30連繫到該伺服器，以便接收並提供無線資料；以及一HTTP內容伺服器(950)，可以一網址10.1.1.31連繫到該伺服器，以便接收並提供有線資料。根據一第二實施例，可以一網址10.1.1.32連繫到的一Apache伺服器(960)可接收並提供無線及有線資料。

圖10示出根據一實施例的一安全系統(1000)。安全系統(1000)包含一前面板介面(1010)。該前面板介面可提供特定實施例所需的所需資訊(例如1011-1018)、資料鏈路(例如1019-1022)、及使用者控制鈕(例如1023-1024)。更具體而言，該等資料鏈路可包括一控制台鏈路(1019)，該控制台包括一顯示裝置(例如監視器)、資料輸入裝置(例如鍵盤)、游標控制裝置(例如滑鼠)、以及可讓使用者設定系統(1000)的組態並監視系統(1000)之其他組件。該等資料鏈路亦可包括：通到一公眾網路或公眾網路介面的一網路鏈路(1021)、以及通到經過安全格式轉換的資料的一目的地之一伺服器鏈路(1022)。這些鏈路可包含超高速乙太網路或RJ45鏈路。

安全系統(1000)亦包含：一匯流排或其他的資訊傳送裝置(1050)，該匯流排(1050)係耦合到前面板介面(1010)，以便傳送資訊；諸如處理器(1060)等的一處理裝置，而該處理器(1060)係耦合到匯流排(1050)，以便處理資料；耦合到匯流排(1050)的一主記憶體(1070)(例如RAM記憶體)，用以儲存資料及處理器(1060)所要執行的指令；耦合到匯流排(1050)的一唯讀記憶體(1080)(例如一BIOS)，用以儲存處理器(1060)的靜態資訊及指令；以及安全防護硬體(1090)。

主記憶體(1070)可儲存選擇指令(1072)及轉換指令(1074)。可在應用程式、模組、資料結構、或其他邏輯中包含該等指令(1072)、(1074)。

根據一實施例，可在硬體中部分地執行安全格式轉換選擇或安全格式轉換。例如，硬體(1090)可包含用來執行模指數運算(modular exponentiation)、虛擬隨機數產生、虛擬隨機金鑰產生、DES/3DES加密及解密、及其他所需安全運算的電路。根據一實施例，硬體(1090)包含用來執行此種安全運算的一加密卡(crypto card)、客戶端可程式閘陣列(Field-Programmable Gate Array；簡稱FPGA)、或特定應用積體電路(Application Specific Integrated Circuit；簡稱ASIC)。

替代實施例

本發明並不限於前文所述之特定實施例，且對此項技術具有一般知識且參閱過本發明揭示事項之人士將可了解

亦可考慮使用許多其他的實施例。

不同的安全格式

根據一第一替代實施例，可配合前文所述的安全格式以外的其他安全格式而使用本發明。該安全格式可以是網際網路工程專門小組(Internet Engineering Task Force；簡稱IETF)所核准的一格式，可以是根據傳輸層安全(Transport Layer Security；簡稱TLS)的一格式，可以是TLS、SSL、或WTLS的一未來強化版本之一格式，或者可以是安全HTTP (S-HTTP)、IP安全(IPSec)、私用通訊技術(Private Communications Technology)、或其他格式等的一格式。

分散式安全系統

根據一第二替代實施例，可將本文所討論的該安全系統分散到多個電腦系統。例如，一第一電腦系統或裝置可以有一選擇系統，一第二電腦系統或裝置可以有一WTLS轉換系統，且一第三電腦系統或裝置可以有一SSL轉換系統。

具有安全系統的伺服器

根據一第三替代實施例，可將一安全系統、一選擇系統、或一轉換系統設於一伺服器中。

網路交換器

根據一第四替代實施例，可將一安全系統、一選擇系統、或一轉換系統設於一具有更大的網路連線能力以提供更佳的連線擴充性之網路交換器中。

推播模式

根據一第五替代實施例，可將一安全系統、一選擇系統、或一轉換系統用於一推播模式中。例如，一資料中心的一伺服器可將平常資料提供給一安全系統，而該安全系統包含一安全格式轉換選擇系統，用以針對一有線裝置而選擇轉換為SSL格式，且針對一無線裝置而轉換為WTLS格式。

身分鑑定

身分鑑定是一系統確認與該系統互動的使用者及電腦的身分之一安全功能及程序。身分鑑定是除了加密之外可實施的一種保證。使用身分鑑定資訊，即可鑑定一裝置之身分。身分鑑定可包括數位憑證、數位簽章、或以上兩者。

在整份說明中，對一來源的身分鑑定係意指對一使用者及(或)一裝置的身分鑑定。此外，身分鑑定係意指證實一用戶端的身分，且確認係意指通常係配合數位憑證程序而執行的一些程序，其中包括(但不限於)：證實數位憑證的有效期間；以及確保數位憑證並未出現在一數位憑證廢止清冊(Certificate Revocation List；簡稱CRL)中。

此外，無線通訊協定(WAP)標準將被用來提供本發明的無線裝置面向中之例子。WAP是一種在行動電話及其他無線終端機上展現並遞送無線資訊及電話服務之全球性標準。自一安全防護的觀點而論，本文中尤其說明了無線傳輸層安全協定(WTLS)，此種協定與用來防護有線互連網

路的安全之安全資料傳輸層(SSL)協定有密切的關聯。

數位憑證

鑑定一裝置的身分之一種方法是利用數位憑證。數位憑證是一種自互連網路下載的資料係來自一聲譽良好的來源之保證。數位憑證利用公開加密技術來確保合法地在連線狀態下轉移機密資訊、資金、或其他敏感性的素材。係由一數位憑證管理機構(Certificate Authority；簡稱CA)核發一數位憑證，且該數位憑證提供了諸如該數位憑證的核發時間及其有效期間等的資訊。

一數位憑證可能在其有效期間屆滿之前即被放棄。例如，該數位憑證可能落入非法機構之手，或者CA可能決定先前所核發的來源已不再是可信賴的。為了拒絕在有效期間屆滿之前即被認定要放棄的數位憑證，CA將被拒絕的數位憑證宣告在一數位憑證廢止清冊(CRL)中。CRL是在數位憑證有效期間屆滿之前即被CA廢止的一份數位憑證清冊，且可自一公用領域(public domain)中取得該CRL。

數位簽章

數位簽章提供了另一種鑑定裝置的身分之方法。數位簽章係用來使用公開金鑰及私密金鑰(private key)來鑑定一簽章者(亦即來源)的身分及所傳輸資訊的完整性。數位簽章的前提是：資料的簽章者具有一私密金鑰，而與該簽章者交換資料的其他人士可能有該簽章者的公開金鑰。其他人士可使用該公開金鑰對資料進行加密或解密，且該簽章者可使用私密金鑰對資料進行加密或解密。

例如，一簽章者可對資料進行雜湊(hashing)，以便產生一訊息摘錄(message digest)，而後以該簽章者的私密金鑰將該訊息摘錄加密，而對一文件執行數位簽章。然後將加密後的訊息摘錄附加到該文件。當一接受者接收到該加密的訊息摘錄及文件時，該接受者使用該簽章者的公開金鑰將加密的訊息摘錄解密，而產生該訊息摘錄。然後對該文件中之資料進行雜湊，並將雜湊值與所產生的訊息摘錄比較，而確認該文件的有效性。如果該雜湊值與該訊息摘錄相符，則確認了該文件的有效性。如果該雜湊值與該訊息摘錄不相符，則該接受者得知該文件中之資料已被竄改，這是因為該雜湊程序並未產生與所傳送的文件相同之訊息摘錄。

PKI/WPKI基礎結構

在所述的本發明實施例中，係參照數位憑證的公開金鑰基礎結構(Public Key Infrastructure；簡稱PKI)及無線公開金鑰基礎結構(Wireless Public Key Infrastructure；簡稱WPKI)系統、數位憑證管理機構、以及證實並鑑定一互連網路交易中涉及的每一方之有效性的其他登錄機構。一般而言，在該PKI/WPKI基礎結構之下，當一裝置要求一數位憑證(後文中稱為"憑證")時，係由一登錄機構核准該憑證，然後將該憑證傳送到一數位憑證管理機構。該數位憑證管理機構然後可核發一憑證。該登錄機構及該數位憑證管理機構通常構成相同的實體。然而，在某些情形中，該登錄機構及該數位憑證管理機構可能是不同的。

概觀

圖11是根據本發明的實施例而建立一安全連線的一方法之一流程圖。該方法開始於步驟(1100)，且繼續進入步驟(1102)，此時一用戶端裝置傳送一用戶端招呼訊息，而要求與一伺服器的一安全連線。在步驟(1104)中，一安全系統代表該伺服器而以一伺服器招呼訊息作為回應，而確認接收到該用戶端裝置的要求。該安全系統然後在步驟(1106)中開始一憑證交換程序，此時決定該用戶端裝置是否(藉由要求一安全連線而)要求身分鑑定。如果該用戶端裝置已要求身分鑑定，則該安全系統在步驟(1108)中傳送身分鑑定資訊。

如果該用戶端裝置並未要求身分鑑定，則該方法跳到步驟(1110)，此時該伺服器亦可要求身分鑑定(亦即，要求該用戶端裝置識別其本身)。如果該伺服器要求身分鑑定，則該用戶端裝置在步驟(1112)中將身分鑑定資訊傳送到該安全系統，並繼續進入步驟(1114)。如果該伺服器並未要求身分鑑定，則該方法跳到步驟(1114)，此時該安全系統將一伺服器招呼已執行訊息傳送到該用戶端裝置，而指示該呼叫連繫的招呼訊息階段已完成。當該用戶端裝置接收到該伺服器招呼已執行訊息時，該用戶端裝置即在步驟(1116)中將一完成訊息傳送到該安全系統，且該安全系統在步驟(1118)中以一完成訊息作為回應。該方法終止於步驟(1120)。

現在已完成了該呼叫連繫，且該用戶端裝置及伺服器可

相互傳送加密的資料，且(或)如果已經傳送了資料，則可使用適於該資料加密所用方法的一解密方法進行解密。

圖12是前文所述基本功能的虛擬碼。該虛擬碼開始於第1行，且在第3行中偵測一加密方法。如果係以WTLS將該資料加密(第5行)，則在第6行中開始一WTLS呼叫連繫。在第7行中，完成了WTLS身分鑑定，且在第8行中將WTLS資料解密。

如果係以SSL將該資料加密(第9行)，則在第10行中開始一SSL呼叫連繫。在第11行中，完成了SSL身分鑑定，且在第12行中將SSL資料解密。如果並未將該資料加密(第13行)，則在第14行中對該資料不執行任何事項。

圖13示出根據本發明一般性實施例的有線及無線身分鑑定之一系統架構(1300)。該系統結構可包含一無線存取裝置(1302)(例如一細胞式電話或一個人數位助理)或一有線存取裝置(1308)(例如一個人電腦瀏覽器)。在一無線存取裝置(1302)的情形中，係利用諸如使用者資料元協定(User Datagram Protocol；簡稱UDP)或無線資料元協定(Wireless Datagram Protocol；簡稱WDP)等的傳輸協定而經由一無線網路(1304)傳送WTLS資料。無線網路(1304)接收該訊息，並將該訊息傳送到WAP閘道器(1306)，且在此處將該傳輸協定自WDP/UDP轉換為TCP/IP，並進行編碼及解碼。

此外，在傳統的方式下，係在該WAP閘道器中將經過WTLS加密的資料轉換為經過SSL加密的資料，且係在該

WAP閘道器上鑑定無線用戶端裝置憑證。然而，此種方式不是一種端點對端點的身分鑑定解決方案。然而，在本發明的實施例中，並不是在該WAP閘道器上進行解密。相反地，係將WTLS資料經由諸如網際網路等的一公眾網路(1310)而傳送到一資料中心(1316)。在一有線存取裝置(1308)的情形中，係將SSL資料經由公眾網路(1310)而直接傳送到資料中心(1316)。

在資料中心(1316)上，鑑定該資料的傳送者(亦即用戶端裝置)之身分，將經過WTLS/SSL加密的資料解密為平常文字，並將該平常文字資料傳送到該資料中心中的許多可能的伺服器(1314)(圖中只示出一個伺服器)中之一個伺服器。資料中心(1316)可包含極像圖3所示安全系統(345)的一安全系統(1312)。

圖13所示之架構(1300)在許多方面都很像圖3所示之架構(300)，但不同之處在於圖13所示之該安全系統在圖3所示的安全系統(345)之上額外地具有一身分鑑定系統。

在圖14所示之一替代實施例中，系統架構(1400)包含一設於WAP伺服器(1306)之前的安全系統(1312)，其中該WAP伺服器(1306)執行WAP閘道器及網路伺服器的功能。在替代實施例中，安全系統(1312)可設於一WAP閘道器之前，而該WAP閘道器之後接續有若干網路伺服器(圖中未示出)。該實施例可包含一防火牆(1402)。例如，某些公司可能針對其應用而在其資料中心中操作其本身的閘道器，因而並不依賴行動服務提供者提供的閘道器服務。

在該實施例中，係利用諸如使用者資料元協定(UDP)或無線資料元協定(WDP)等的傳輸協定而將WTLS資料自一無線裝置(1302)傳送到一無線網路(1304)。無線網路(1304)接收該訊息，且經由公眾網路(1310)而繞送該資料，然後該資料經過防火牆(1402)。

一旦在安全系統(1312)上接收到該資料之後，安全系統(1312)即鑑定經過WTLS加密的資料，且若適用，則將該經過WTLS加密的資料轉換為平常文字。安全系統(1312)然後進行身分鑑定。在一有線存取裝置(1308)的情形中，係將SSL資料經由公眾網路(1310)而傳送到資料中心(1316)，此時安全系統(1312)即鑑定經過SSL加密的資料，且若適用，則將該經過SSL加密的資料轉換為平常文字。然後將該平常文字資料傳送到該資料中心中的許多可能的伺服器(1314)(圖中只示出一個伺服器)中之一個伺服器。

安全系統(1312)維護一CRL，且係按照預定的時間間隔利用由CA更新的一可公開存取之CRL來更新其所維護的該CRL。該安全系統利用可公開存取之CRL來更新其CRL，且包含一身分鑑定系統，用以將其自用戶端裝置接收的用戶端憑證與其CRL比較，而決定該等憑證是否有效。

諸如當用戶端裝置要求身分鑑定時，安全系統(1312)亦要求將伺服器端憑證傳送到用戶端裝置。安全系統(1312)維護定期的憑證，以便傳送到有線裝置，並維護長期及點其的憑證，以便傳送到無線用戶端裝置。有線裝置

可將一伺服器的憑證與該有線裝置所維護的一CRL比對，而鑑定該伺服器的身分。

在無線用戶端裝置的情形中，因為無線裝置沒有本機資源或通訊頻寬來實施諸如CRL等的廢止方法，所以在一段較長的期間中鑑定伺服器的身分一次(亦即，核發一長期憑證)，且在可對用戶端裝置發出的整個該段較長的期間中對伺服器核發短期憑證。伺服器又將一長期憑證及一短期憑證傳送到用戶端裝置，而這兩個憑證都必須是有效的，以供用戶端裝置鑑定該伺服器的身分。

如果CA想要廢止該伺服器，CA只須停止將新的短期憑證核發給該伺服器。因此，如果該短期憑證是無效的，則不會再將一目前有效的憑證提供給用戶端裝置，因而該用戶端裝置將不會把該伺服器視為通過身分鑑定。此種方式使用戶端裝置不太需要維護一CRL來比對伺服器端憑證。

伺服器端憑證支援

伺服器身分鑑定可讓用戶端裝置利用伺服器憑證來鑑定伺服器的身分，且只讓具有有效伺服器憑證的伺服器與一用戶端裝置連線。係由一CA(例如位於Mountain View, California的VeriSign)核發伺服器憑證，而該CA在核發一伺服器憑證之前，先檢查該伺服器憑證的申請人是否符合該CA的可信賴準則。該伺服器憑證可讓一伺服器與一用戶端裝置連線，直到該伺服器憑證的有效期間屆滿為止。在屆滿之後，將封鎖該伺服器。為了要重新可連線，該CA必須重新確認該伺服器的可信賴性。

然而，在一伺服器憑證的有效期間屆滿之前，可能會放棄該伺服器憑證。有線裝置可維護一CRL，以便鑑定伺服器的身分，另一方面係將短期憑證發給無線裝置。

圖15示出伺服器端憑證針對有線裝置及無線用戶端裝置的一作業流程(1500)。一安全系統(1312)向一數位憑證管理機構(1502)要求伺服器憑證，且該數位憑證管理機構將該伺服器憑證放入一憑證儲存單元(1504)中，而係在該憑證儲存單元(1504)中維護憑證資訊(其中包括憑證編號及憑證所核發的對象)。

一用戶端裝置(1302)、(1308)可經由安全系統(1312)而連接到資料中心(1316)中之一伺服器(1314)。一無線存取裝置(1302)將一WTLS訊息傳送到一無線網路(1304)，而嘗試與該伺服器間之一安全連線(該安全連線必然是一對身分鑑定的要求(有時被稱為"身分鑑定要求"))。無線網路(1304)將該訊息傳送到一WAP閘道器(1306)，而一有線存取裝置(1308)則可經由公眾網路(1310)而直接連接。該WAP閘道器(1306)然後將加密後的用戶端訊息經由一公眾網路(1310)而傳送到安全系統(1312)。安全系統(1312)回應該用戶端裝置對身分鑑定的要求，而將一伺服器憑證傳送到該用戶端裝置(1302)、(1308)。用戶端裝置(1302)、(1308)然後可鑑定該伺服器憑證。

圖16是根據本發明一般性實施例的伺服器端憑證的一方法之一流程圖。該發法開始於步驟(1600)，且繼續進入步驟(1602)，此時一安全系統向一CA要求伺服器憑證，

且該CA在步驟(1604)中將該等憑證傳送到該安全系統。在步驟(1606)中，該安全系統諸如回應要求身分鑑定的一用戶端裝置，而將一伺服器憑證傳送到該用戶端裝置。在步驟(1608)中，決定該伺服器憑證是否有效。如果該伺服器憑證是有效的，則在步驟(1610)中建立一安全連線。否則，該用戶端裝置在步驟(1612)中關閉該連線。該方法終止於步驟(1614)。

該安全系統可按照使用者鑑定的時間間隔輪詢該憑證儲存單元，以便：取得憑證，更新短期及長期憑證，且(或)更新其CRL。

*無線用戶端裝置

在無線互連網路中，一WTLS伺服器憑證是一用來向一無線裝置鑑定一伺服器的身分之憑證。當一無線裝置使用者想要將機密資料傳送到一伺服器時，該WAP裝置將要求該伺服器的數位憑證。該無線裝置使用其中包含該WAP伺服器的公開金鑰之該憑證執行下列各事項：

* 鑑定該伺服器的身分；以及
* 利用WTLS協定將提供給該伺服器的資訊加密。

然而，該WPKI架構涉及一不同的實施方式，這是因為一WAP裝置很難為了檢查伺服器端憑證是否已被廢止而持續地更新該CRL清冊。在該WPKI架構中，該安全系統維護短期憑證及長期憑證。使用者可規定要求的時間間隔。

圖17是根據本發明實施例的伺服器端憑證針對無線用

戶端裝置的一方法之一流程圖。該方法開始於步驟(1700)，且繼續進入步驟(1702)，此時一安全系統代表該伺服器向一CA要求伺服器憑證(其中包括短期及長期憑證的下載及更新)。因為可根據使用者規定的時間間隔而要求伺服器憑證，所以並不必然每次都要執行該步驟。

在步驟(1704)中，該CA將伺服器憑證傳送到該安全系統。在步驟(1706)中，將一長期憑證及一短期憑證傳送到用戶端裝置。例如，可回應一用戶端裝置對身分鑑定的要求，而將該伺服器憑證傳送到該用戶端裝置。

在步驟(1708)中，驗證該CA的數位簽章及該憑證的有效期間，而決定該伺服器憑證是否有效。如果長期及短期憑證都仍然有效，則在步驟(1710)中建立一安全連線。否則，該用戶端裝置可在步驟(1712)中關閉該連練。該方法終止於步驟(1714)。

*有線用戶端裝置

同樣地，在有線互連網路中，SSL憑證是一種用來向一有線裝置(亦即個人電腦)鑑定一伺服器的身分之憑證。

為了拒絕在有效期間屆滿之前即被認定要放棄的伺服器憑證，一用戶端裝置查詢一憑證廢止清冊(CRL)，而係在一公用領域中維護該CRL，且可將該CRL下載到該用戶端裝置。如果在該CRL中發現該伺服器憑證，則該用戶端裝置通常將關閉該連線。

圖18是根據本發明實施例的伺服器端憑證針對有線用戶端裝置的一方法之一流程圖。該方法開始於步驟(1800)

，且繼續進入步驟(1802)，此時一安全系統代表該伺服器向一CA要求伺服器憑證。在步驟(1804)中，該CA將伺服器憑證傳送到該安全系統。在步驟(1806)中，將一伺服器憑證傳送到用戶端裝置。例如，可回應一用戶端裝置對身分鑑定的要求，而將該伺服器憑證傳送到該用戶端裝置。

在步驟(1808)中，該用戶端裝置決定該伺服器憑證是否在該CRL中，而驗證該伺服器憑證。如果該伺服器憑證不在該CRL中，則在步驟(1810)於該用戶端裝置與該伺服器之間建立一安全連線。否則，該用戶端裝置在步驟(1812)中關閉該連線。該方法終止於步驟(1814)。

伺服器端憑證支援

用戶端裝置身分鑑定可使用被安裝在使用者的網路瀏覽器或其他用戶端裝置應用程式之用戶端裝置憑證來鑑定使用者的身分，且只讓具有有效用戶端裝置憑證的用戶端裝置進入一授權領域(亦即，諸如一網站上的一限制區域)。係由一數位憑證管理機構(CA)核發用戶端裝置憑證。該CA在核發一用戶端裝置憑證之前，先檢查該用戶端裝置憑證的申請人是否符合該CA的可信賴準則。該用戶端裝置憑證可讓一用戶端裝置進入該授權領域，直到該用戶端裝置憑證的有效期間屆滿為止。在屆滿之後，將封鎖該使用者。為了要重新進入該授權領域，該CA在更新該用戶端裝置憑證之前，必須重新確認該使用者的可信賴性。藉由檢查用戶端裝置憑證的核發日期及更新日期，將有助於確保唯有可被信賴進入一授權領域的使用者才持有

有效的用戶端裝置憑證。

然而，在一用戶端裝置憑證有效期間屆滿之前，可能會放棄該用戶端裝置憑證。例如，其他的人可能非法取得該用戶端裝置憑證，或者該CA可能決定其先前核發用戶端裝置憑證的使用者已不再是可被信賴。如果一用戶端裝置憑證在其有效期間屆滿之前即被放棄，則該CA可將該被廢止的用戶端裝置憑證加入一憑證廢止清冊(CRL)中。係由該CA維護該CRL，但可將該CRL下載到伺服器，以便鑑定用戶端裝置的身分。

為了拒絕有效期間屆滿之前即被認定要放棄的用戶端裝置憑證，一伺服器查詢一憑證廢止清冊(CRL)，而係在一公用領域中維護該CRL，且可將該CRL下載到伺服器。如果被廢止的用戶端裝置憑證在該CRL中，則具有被廢止的用戶端裝置憑證之用戶端裝置將被拒絕進入一授權領域。

在本發明之實施例中，安全系統(1312)支援CRL。安全系統(1312)自該公用領域下載該CRL。當回應一伺服器對身分鑑定的要求而接收到一用戶端裝置憑證時，即將該用戶端裝置憑證與該伺服器的CRL比對，以便決定該用戶端裝置憑證是否已被廢止。

在本發明之實施例中，該安全系統可代表伺服器而起動或停止藉由用戶端憑證而進行之身分鑑定。例如，可針對諸如股票報價下單等的交易而起動身分鑑定，但是可針對諸如服務平常網頁等的交易而停止身分鑑定。

圖19示用戶端憑證針對有線及無線用戶端裝置的一作業流程(1900)。一無線用戶端裝置(1302)經由一無線網路(1902)連接到一CA(1502)，而申請一憑證。CA(1502)核發該憑證，並將該憑證放入憑證儲存單元(1504)。CA(1502)然後將一用戶端裝置憑證或一憑證URL傳送到該用戶端裝置，且該用戶端裝置(1302)可嘗試使用一WTLS訊息及該用戶端裝置憑證或該用戶端裝置憑證的一連結，而連接到伺服器(1314)。

安全系統(1312)按照使用者規定的時間間隔而更新其CRL。該安全系統將該WTLS訊息解密，並將解密後的WTLS訊息與該CRL比對，而檢查是否為一有效的用戶端裝置憑證。如果該用戶端裝置憑證是有效的，則建立一安全連線。否則，該伺服器可選擇關閉該連線，或者容許該連線，但是諸如拒絕該用戶端裝置進入一授權領域。

對於該有線用戶端裝置(1308)而言，係經由公眾網路(1310)(亦即網際網路)向數位憑證管理機構(1502)要求一用戶端裝置憑證。一有線用戶端裝置(1308)可傳送一SSL訊息及一用戶端裝置憑證，而嘗試連接到伺服器(1314)。如果該用戶端裝置憑證是有效的，則建立一安全連線。否則，該伺服器可選擇關閉該連線，或者容許該連線，但是諸如拒絕該用戶端裝置進入一授權領域。

圖20是根據本發明一般性實施例而用於有線用戶端裝置憑證針的一方法之一流程圖。該方法開始於步驟(2000)，且繼續進入步驟(2002)，此時一用戶端裝置申請有線用

戶端裝置憑證。在步驟(2004)中，一數位憑證管理機構將有線用戶端裝置憑證核發給該用戶端裝置。在步驟(2006)中，該用戶端裝置可在沒有該有線用戶端裝置憑證的情形下要求一安全連線，且在步驟(2008)中，係回應該伺服器對用戶端裝置身分鑑定之要求，而將該有線用戶端裝置憑證傳送到該伺服器。

在步驟(2010)中，一安全系統代表該伺服器驗證該有線用戶端裝置憑證。如果該憑證是有效的，則在步驟(2012)中建立一安全連線。否則，在步驟(2014)中不建立一安全連線，且該伺服器可選擇關閉該連線，或者容許該連線，但是諸如拒絕該用戶端裝置進入一授權領域。該方法終止於步驟(2016)。

*無線用戶端裝置

在無線互連網路中，係將一WTLS用戶端裝置憑證用來向一伺服器鑑定一無線裝置的身分。舉例而言，係將WTLS用戶端裝置憑證界定為WAP 1.2的一部分，並將WTLS用戶端裝置憑證格式化為諸如X.509憑證或小型憑證(mini-certificate)。

圖21是根據本發明實施例的用於無線用戶端憑證針的一方法之一流程圖。該方法開始於步驟(2100)，且繼續進入步驟(2102)，此時一用戶端裝置申請一無線用戶端裝置憑證。在步驟(2104A)中，該CA產生該無線用戶端裝置憑證的一通用資源位標(URL)，並將該憑證的URL傳送到該用戶端裝置。在替代實施例中，可在步驟(2104B)中將該

CA所核發的一無線用戶端裝置憑證傳送到用戶端，並將該無線用戶端裝置憑證儲存在WAP裝置的一無線身分模組(Wireless Identity Module；簡稱WIM)。係將WIM用來執行WTLS及應用層級的安全功能，且係用來儲存及處理使用者識別及身分鑑定所需的資訊。

該用戶端裝置可在步驟(2106)中嘗試一安全連線，然後在步驟(2108)中回應該伺服器對身分鑑定的要求，而傳送用戶端裝置憑證(或該憑證的連結)。該安全系統將該WTLS訊息解密，並在步驟(2110)中將解密後的WTLS訊息與一CRL比對，以便決定該用戶端裝置憑證是否有效。如果該用戶端裝置憑證是有效的，則在步驟(2112)中於該用戶端裝置與該伺服器之間建立一安全連線。否則，在步驟(2114)中不建立一安全連線，且該伺服器可選擇關閉該連線，或者容許該連線，但是不讓該用戶端裝置進入一授權領域。該方法終止於步驟(2116)。

*有線用戶端裝置

在有線互連網路中，SSL用戶端裝置憑證是一種用來向一伺服器鑑定一有線裝置的身分之用戶端裝置憑證。圖22是根據本發明實施例的用於有線用戶端憑證針的一方法之一流程圖。

該方法開始於步驟(2200)，且繼續進入步驟(2202)，此時一用戶端裝置申請一有線用戶端裝置憑證。在步驟(2204)中，該CA核發該憑證，並將該憑證傳送到該用戶端裝置。在步驟(2206)中，該用戶端裝置嘗試與該伺服器

間之一安全連線，然後在步驟(2208)中回應該伺服器對身分鑑定的要求，而傳送該有線用戶端裝置憑證。

在步驟(2208)中，該安全系統將該SSL訊息解密，並將用戶端裝置憑證與一CRL比對，以便決定該用戶端裝置憑證是否有效。如果該用戶端裝置憑證是有效的，則在步驟(2212)中於該用戶端裝置與該伺服器之間建立一安全連線。否則，在步驟(2214)中不建立一安全連線，且該伺服器可選擇關閉該連線，或者容許該連線，但是不讓該用戶端裝置進入一授權領域。該方法終止於步驟(2216)。

*數位簽章

除了傳送一用戶端裝置憑證之外，一用戶端裝置可傳送一數位簽章。如果一用戶端裝置傳送一數位簽章，則係由伺服器驗證該數位簽章。如果該數位簽章是有效的，則建立一安全連線。否則，拒絕該用戶端裝置進入該授權領域。

對於無線用戶端裝置而言，可諸如利用可用的WAP功能來實施數位簽章。WAP 1.2亦界定了不是WTLS的一部分的一基於WPKI之功能。該功能可讓一WAP用戶端裝置對一交易進行數位簽章，且係將該功能稱為無線標記語言(WML)的描述語言程式簽章文字功能(Script Sign Text Function)，且該功能係針對需要來自用戶端的非著名簽章之應用。

安全系統

圖23示出安全系統的一架構。該安全系統(2300)包含一

應用模組(2302)、SSL模組(2304)、PKI模組(2308)、WTLS模組(2306)、及WPKI模組(2310)。該安全系統的輸入包含送入的資料(2314)，該送入的資料(2314)可以是經過SSL加密的資料、經過WTLS加密的資料、或平常資料。該安全系統的輸出是平常資料(2316)，然後可由一伺服器處理該平常資料(2316)。

應用模組(2302)偵測送入的資料(2314)是經過SSL加密的、或經過WTLS加密的、或平常文字。應用模組(2302)然後代表在其後面的該等伺服器處理WTLS/SSL呼叫連繫，並與PKI/WPKI模組互動，以便進行伺服器及用戶端身分鑑定。

如果送入的資料(2314)是經過SSL加密的，且已確定了身分鑑定，則該應用模組呼叫SSL模組(2304)。SSL模組(2304)讀取該資料，並將該資料解密為平常資料(2316)。當該SSL模組(2304)完成了其程序時，即執行應用模組(2302)。SSL模組(2304)可將一硬體加密卡用於SSL功能，且該加密卡提供了SSL加速。該SSL模組可包含圖3所示之SSL轉換系統(374)。在本發明的一般性實施例中，SSL模組(2304)可以是一有線裝置解密模組，該模組利用一有線安全協定而接收加密的資料(亦即經過SSL加密的資料)，並將此種資料解密為平常文字。

如果應用模組(2302)偵測到經過WTLS加密的資料，且已確定了身分鑑定，則呼叫WTLS模組(2306)。WTLS模組(2306)讀取送入的資料(2314)，並將該資料解密為平常文

字(2316)。當WTLS模組(2306)圍成其程序時，即執行應用模組(2302)。WTLS模組(2306)可以是純粹的軟體、或軟體及硬體的一組合。可執行該硬體中的經常佔用處理器之功能，而加速WTLS加密及解密。該WTLS模組可包含圖3所示之WTLS轉換系統(372)。在本發明的一般性實施例中，WTLS模組(2306)可以是一無線裝置解密模組，該模組利用一無線安全協定而接收加密的資料(亦即經過WTLS加密的資料)，並將此種資料解密為平常文字。

PKI模組(2308)具有驗證數位簽章及(或)鑑定有線用戶端裝置憑證的功能，而鑑定有線用戶端裝置憑證的功能之方式係檢查其CRL，以確定是否有任何已被該CA廢止的用戶端裝置憑證。係按照使用者規定的時間間隔，利用對LDAP伺服器的一LDAP/FTP/HTTP要求來更新該CRL清冊。PKI模組(2308)藉由自一CA下載伺服器端憑證，並將該等憑證發給各用戶端裝置，而亦支援伺服器的身分鑑定。在本發明的一般性實施例中，PKI模組(2308)可以是一有線裝置身分鑑定模組，而該模組接收有線身分鑑定資訊，並利用該有線身分鑑定資訊來鑑定有線裝置的身分。

WPKI模組(2310)具有驗證無線數位簽章及(或)鑑定無線用戶端裝置憑證的功能，而鑑定無線用戶端裝置憑證的功能之方式係檢查其CRL，以確定是否有任何已被該CA廢止的用戶端裝置憑證。係按照使用者規定的時間間隔，利用對LDAP伺服器的一輕量級目錄存取協定(Lightweight Directory Access Protocol；簡稱LDAP)/檔

案傳輸協定(File Transfer Protocol；簡稱FTP)/超文件傳輸協定(HyperText Transfer Protocol；簡稱HTTP)要求來更新該CRL清冊。在本發明的一般性實施例中，WPKI模組(2310)可以是一無線裝置身分鑑定模組，而該模組接收無線身分鑑定資訊，並利用該身分鑑定資訊來鑑定無線裝置的身分。

WPKI模組(2310)亦支援利用伺服器端憑證來鑑定伺服器的身分。有兩類由該模組處理的伺服器端憑證。可將短期憑證的有效期間設定為每隔24小時即屆滿，且可將長期憑證的有效期間設定為在一年後屆滿。係按照使用者規定的時間間隔，而自一CA更新(亦即下載)該等憑證。

其他模組

一旦該應用模組自SSL模組(2304)或WTLS模組(2306)取得送入的資料(2314)之後，即可呼叫諸如XML處理模組、負載平衡模組、或XML變換模組等的其他模組(2312)，以便提供與網路裝置有關的其他功能。可將該等其他模組與諸如基於內容的切換、基於XML的路由、及裝置偵測等的功能結合。

組態設定

圖24示出設定一安全系統的組態的方式之一個例子。各欄位的定義係如下文所示：

* 連線圖識別碼提供一連線的一任意識別碼；
* 連線類型欄位提供諸如安全連線或不安全連線等的連線類型、以及加密類型(亦即SSL或WTLS)；

* 密鑰識別碼欄位提供安全連線所用的密鑰識別碼；
* 伺服器IP欄位提供用來與資料中心中的各伺服器通訊之一網際網路協定位址；
* 網路埠欄位提供可用來自一公眾網路接收安全資料或不安全的資料之預定的習知埠編號；
* 伺服器埠欄位提供可用來將平常資料傳送到資料中心中的伺服器之一習知的預定埠；
* 密碼套件欄位存放安全連線及不安全連線所用的安全強度之一指示；
* 重新導向欄位提供在一存取裝置不支援所使用的安全特性時將該裝置重新導向安全升級資源之一選項；
* 用戶端裝置身分鑑定欄位決定是否要求利用數位憑證進行用戶端裝置身分鑑定；
* 數位簽章欄位決定是否要求利用數位簽章進行用戶端裝置身分鑑定。

可利用圖形使用者介面(Graphical User Interface；簡稱GUI)或通用語言介面(Common Language Interface；簡稱CLI)來執行一安全系統的組態設定。例如，可利用一CLI而自安全防護系統供應商取得用戶端裝置憑證及伺服器憑證。可利用CLI來設定CRL的更新時間。可利用超文件傳輸協定(HTTP)、檔案傳輸協定(FTP)、或LDAP要求而自一LDAP伺服器更新CRL清冊。亦可按照使用者規定的時間間隔，而自動地自CA儲存單元更新短期伺服器憑證。如果用戶端裝置不支援伺服器端上所需的安全功能，則利

用該重新導向參數將該用戶端裝置重新導向到具有所需安全相關資訊之一URL。

在前文的說明書中，已參照本發明的特定實施例而說明了本發明。然而，顯然可在不脫離本發明的廣義精神及範圍下，對本發明作出各種修改及改變。因此，應將本說明書及各圖式視為舉例說明，而非對本發明加以限制。

例如，雖然在本說明書中說明了PKI/WPKI及SSL/WTLS協定，但是對此項技術具有一般知識者當可了解，係為了舉例說明而述及這些協定，且不應將這些協定視為對本發明加以限制。因此，亦可使用其他的協定。

圖式簡單說明

係以舉例說明之方式解說本發明，且這些例子並未對本發明加以限制，而在各附圖中，相同的代號係表示類似的元件，這些附圖有：

圖1示出根據一實施例的在一資料中心中之一安全系統。

圖2示出根據一實施例的一WAP堆疊。

圖3示出根據一實施例的一系統架構。

圖4示出根據一實施例而操作一安全系統之一方法。

圖5示出根據一實施例的一WTLS安全協定架構。

圖6示出根據一實施例的一WTLS呼叫連繫。

圖7示出根據一實施例的一用戶端招呼訊息。

圖8示出根據一實施例的安全系統。

圖9示出根據一實施例的一資料中心之架構。

圖10示出根據一實施例的一安全系統。

圖11是根據本發明一般性實施例而在一用戶端裝置與一伺服器之間建立一呼叫連繫的一方法之一流程圖。

圖12示出根據本發明一般性實施例而在一用戶端裝置與一伺服器之間建立一呼叫連繫的虛擬碼。

圖13示出根據本發明一般性實施例的有線及無線身分鑑定之一系統架構。

圖14示出根據本發明一般性實施例的有線及無線身分鑑定之一替代性系統架構。

圖15示出伺服器端憑證針對有線及無線用戶端裝置的一作業流程。

圖16是根據本發明一般性實施例的一伺服器端憑證方法之一流程圖。

圖17是針對無線用戶端裝置的一伺服器端憑證方法之一流程圖。

圖18是針對有線用戶端裝置的一伺服器端憑證方法之一流程圖。

圖19示出伺服器端憑證針對有線及無線用戶端裝置的一作業流程。

圖20是根據本發明一般性實施例的一用戶端端憑證方法之一流程圖。

圖21是針對無線用戶端裝置的一用戶端憑證方法之一流程圖。

圖22是針對有線用戶端裝置的一用戶端憑證方法之一流程圖。

圖23示出根據本發明一般性實施例的一安全系統。

圖24示出一安全系統的一例示組態設定。

圖式代表符號說明

100	安全的通訊系統
110	網路存取裝置
120，325，1310	公眾網路
130	安全格式指示
140	安全資料
150，340，900，1316	資料中心
160，345，920，1000，1312，2300	安全系統
170，360，800	選擇系統
180，370	轉換系統
190	埠
131	安全特性
200	WAP堆疊
210	應用層
220	交談層
230	交易層
240	安全層
250	傳輸層
260	網路層
300，1300，1400	系統架構
305，1302	無線存取裝置
320，1308	有線存取裝置

310，1304，1902	無線網路
315，1306	WAP閘道器
330，335，810	指示
390，940-960，1314	伺服器
350	網路介面
380	第二網路介面
354	第一及第二埠
352	第二及第三埠
372	WTLS轉換系統
374	SSL轉換系統
385	其他的組件
500	WTLS安全架構
550	記錄協定
510	呼叫連繫協定
520	警示協定
530	應用協定
540	改變密碼規格協定
600	WTLS呼叫連繫
610	無線存取用戶端裝置
670	資料中心伺服器
700	用戶端招呼訊息
710	用戶端裝置安全能力資訊
720	隨機結構資訊

730	交談識別碼資訊
740	支援的密碼選項資訊
750	壓縮方法資訊
812	埠資訊
814	安全特性資訊
820	協定選擇邏輯
830	協定選擇
840	安全特性選擇邏輯
850	無線邏輯部分
860	有線邏輯部分
870	安全格式轉換選擇
910，930	交換器/路由器
1010	前面板介面
1011-1018	所需資訊
1019-1022	資料鏈路
1023-1024	使用者控制鈕
1050	匯流排
1060	處理器
1070	主記憶體
1080	唯讀記憶體
1090	安全防護硬體
1072	選擇指令
1074	轉換指令
1402	防火牆

1500、1900	作業流程
1502	數位憑證管理機構
1504	憑證儲存單元
2302	應用模組
2304	SSL模組
2308	PKI模組
2306	WTLS模組
2310	WPKI模組
2314	送入的資料
2316	平常資料
2312	其他模組

拾、申請專利範圍

1. 一種方法，包含下列步驟：

將一訊息自一用戶端裝置傳送到一伺服器，該訊息係用來建立一安全連線；

與該伺服器相關聯的一安全系統攔截該資料，以便執行各身分鑑定功能；以及

如果執行了適當的身分鑑定，則建立一安全連線。

2. 如申請專利範圍第1項之方法，其中該適當的身分鑑定包含下列步驟：如果該用戶端裝置已要求身分鑑定，則決定該伺服器是否為可信賴的。

3. 如申請專利範圍第2項之方法，其中該適當的身分鑑定又包含下列步驟：如果該伺服器已要求身分鑑定，則決定該用戶端裝置是否為可信賴的。

4. 如申請專利範圍第1項之方法，其中該適當的身分鑑定包含下列步驟：確認數位憑證。

5. 如申請專利範圍第1項之方法，又包含下列步驟：如果該訊息被加密，則將該訊息解密。

6. 如申請專利範圍第1項之方法，其中該身分鑑定功能包含下列步驟：

該伺服器向該用戶端裝置要求身分鑑定；

自該用戶端裝置接收一用戶端裝置憑證；以及

決定該用戶端裝置是否為可信賴的，且係在代表該伺服器的該安全系統上執行該決定步驟。

7. 如申請專利範圍第6項之方法，其中該訊息包含一用來

確認該用戶端裝置的身分之數位簽章，且執行該適當的身分鑑定之該步驟包含下列步驟：確認該數位簽章。

8. 一種方法，包含下列步驟：

在與一伺服器相關聯的一裝置上接收來自一用戶端裝置的用戶端招呼訊息，該用戶端招呼訊息指示與該伺服器建立一安全連線的一要求；

該裝置回應該用戶端招呼訊息，而代表該伺服器傳送一伺服器招呼訊息，以便確認接收到該用戶端招呼訊息；

如果該用戶端裝置及該伺服器的至少其中之一要求身分鑑定，則交換身分鑑定資訊；

將一伺服器招呼已執行訊息自該裝置傳送到該用戶端裝置，且係代表該伺服器而執行該傳送步驟；

自該用戶端裝置接收一完成訊息；以及

將一完成訊息自該裝置傳送到該用戶端裝置，且係代表該伺服器而執行該傳送步驟。

9. 如申請專利範圍第8項之方法，其中該交換身分鑑定資訊步驟包含下列步驟：

如果該用戶端招呼訊息包括對該伺服器的身分鑑定之一要求，則代表該伺服器將身分鑑定資訊自該裝置傳送到該用戶端裝置；以及

如果該伺服器向該用戶端裝置要求身分鑑定，則自該用戶端裝置接收身分鑑定資訊。

10. 如申請專利範圍第8項之方法，其中代表該伺服器將一完成訊息自該裝置傳送到該用戶端裝置之該步驟包含下列步驟：

決定該用戶端裝置是否為可信賴的；以及

如果已鑑定了該用戶端裝置的身分，則在該用戶端裝置與該伺服器之間建立一安全連線。

11. 如申請專利範圍第10項之方法，其中該身分鑑定資訊包含一用戶端裝置憑證，且決定該用戶端裝置是否為可信賴的該步驟包含下列步驟：確認該用戶端裝置憑證。

12. 如申請專利範圍第11項之方法，其中確認該用戶端裝置憑證之該步驟包含下列步驟：決定該用戶端裝置憑證不在一數位憑證廢止清冊中。

13. 如申請專利範圍第11項之方法，其中該身分鑑定資訊又包含一數位簽章，且決定該用戶端裝置是否為可信賴的該步驟又包含下列步驟：驗證該數位簽章。

14. 如申請專利範圍第8項之方法，又包含下列步驟：如果該訊息被加密，則將該訊息解密。

15. 一種裝置，包含：

一應用模組，該應用模組係用來執行下列步驟：

接收一用戶端裝置所傳送的且目的地為一資料中心的複數個伺服器中之一特定伺服器之送入的資料；以及

將該資料繞送到一身分鑑定模組，以便確認該用戶

端裝置之身分；

與該等複數個伺服器相關聯的一有線裝置身分鑑定模組，該有線裝置身分鑑定模組係用來執行下列步驟：

如果係利用有線身分鑑定資訊來傳送該送入的資料，則自該應用模組接收該送入的資料；以及

鑑定該有線裝置的身分；

與該等複數個伺服器相關聯的一無線裝置身分鑑定模組，該無線裝置身分鑑定模組係用來執行下列步驟：

如果係利用無線身分鑑定資訊來傳送該送入的資料，則自該應用模組接收該送入的資料；以及

鑑定該無線裝置的身分；

與該等複數個伺服器相關聯的一有線裝置解密模組，該有線裝置解密模組係用來執行下列步驟：

如果係使用一有線安全協定將該送入的資料加密，則自該應用模組接收該送入的資料；以及

將該資料解密為平常文字；以及

與該等複數個伺服器相關聯的一無線裝置解密模組；該無線裝置解密模組係用來執行下列步驟：

如果係使用一無線安全協定將該送入的資料加密，則自該應用模組接收該送入的資料；以及

將該資料解密為平常文字。

16. 如申請專利範圍第15項之裝置，其中該有線裝置身分

鑑定模組及該無線裝置身分鑑定模組又支援一些身分鑑定功能，以便以下列的步驟來鑑定特定伺服器的身分：

向一數位憑證管理機構要求伺服器憑證；

儲存該等伺服器憑證；以及

回應一用戶端裝置對身分鑑定的要求，而將至少一個該等伺服器憑證傳送到該用戶端裝置。

17. 如申請專利範圍第16項之裝置，其中該用戶端裝置是一無線用戶端裝置，且該傳送步驟包含下列步驟：將一長期憑證及一短期憑證傳送到該無線用戶端裝置。

18. 如申請專利範圍第16項之裝置，其中向該數位憑證管理機構要求伺服器憑證之該步驟包含下列步驟：按照使用者規定的時間間隔而要求該等伺服器憑證。

19. 一種系統，包含：

一個或多個伺服器，用以與各用戶端裝置交換資料；以及

與該等一個或多個伺服器相關聯的一安全系統，該安全系統係用來執行下列步驟：

支援一些身分鑑定功能，以便鑑定該等一個或多個伺服器之身分；以及

鑑定要求與該等一個或多個伺服器建立一安全連線的各用戶端裝置之身分。

20. 如申請專利範圍第19項之系統，其中用來鑑定該等一個或多個伺服器的身分之該等身分鑑定功能包含下列

步驟：

向一數位憑證管理機構要求伺服器憑證；以及

回應一用戶端裝置對該等一個或多個伺服器中的一個伺服器身分鑑定之要求，而將一伺服器憑證傳送到該用戶端裝置。

21. 如申請專利範圍第19項之系統，其中鑑定要求與該等一個或多個伺服器建立一安全連線的各用戶端裝置之身分之該步驟包含下列步驟：

更新一數位憑證廢止清冊(CRL)；

自一要求與該安全系統相關聯的該等一個或多個伺服器中的一特定伺服器建立一安全連線之一用戶端裝置接收一用戶端裝置憑證；

決定該用戶端裝置憑證是否在該CRL中；以及

如果該用戶端裝置憑證在該CRL中，則拒絕該用戶端裝置存取該特定伺服器。

22. 一種裝置，包含：

一第一裝置，該第一裝置係用來執行下列步驟：

接收一用戶端所傳送的且目的地為一資料中心的複數個伺服器中之一特定伺服器之送入的資料；以及

將該資料繞送到一確認裝置，該確認裝置鑑定與該用戶端相關聯的一裝置之身分，而確認該用戶端之身分；

一第二裝置，該第二裝置係用來執行下列步驟：

如果係利用有線身分鑑定資訊來傳送該送入的資料

，則自該第一裝置接收該送入的資料；以及

鑑定該有線裝置的身分；

一第三裝置，該第三裝置係用來執行下列步驟：

如果係利用無線身分鑑定資訊來傳送該送入的資料，則自該第一裝置接收該送入的資料；以及

鑑定該無線裝置的身分；

一第四裝置，該第四裝置係用來執行下列步驟：

如果係使用一有線安全協定將該送入的資料加密，則自該第一裝置接收該送入的資料；以及

將該資料解密為平常文字；以及

一第五裝置，該第五裝置係用來執行下列步驟：

如果係使用一無線安全協定將該送入的資料加密，則自該第一裝置接收該送入的資料；以及

將該資料解密為平常文字。

23. 如申請專利範圍第22項之裝置，其中該第二及第三裝置又支援一些身分鑑定功能，以便以下列的步驟來鑑定特定伺服器的身分：

向一數位憑證管理機構要求伺服器憑證；

儲存該等伺服器憑證；以及

回應一用戶端裝置對身分鑑定的要求，而將至少一個該等伺服器憑證傳送到該用戶端裝置。

24. 如申請專利範圍第23項之裝置，其中該用戶端裝置是一無線用戶端裝置，且該傳送步驟包含下列步驟：將一長期憑證及一短期憑證傳送到該無線用戶端裝置。

25. 如申請專利範圍第23項之裝置，其中向該數位憑證管理機構要求伺服器憑證之該步驟包含下列步驟：按照使用者規定的時間間隔而要求該等伺服器憑證。

26. 一種機器可讀取之媒體，該機器可讀取之媒體中儲存有用來代表指令序列的資料，而當一處理器執行該等指令序列時，將使該處理器執行下列步驟：

接收自一用戶端裝置傳送到一伺服器之訊息，該訊息係用來建立一安全連線；

在與該伺服器相關聯的一安全系統上攔截該資料，以便執行各身分鑑定功能；以及

如果執行了適當的身分鑑定，則建立一安全連線。

27. 如申請專利範圍第26項之機器可讀取之媒體，其中該適當的身分鑑定包含下列步驟：如果該用戶端裝置已要求身分鑑定，則決定該伺服器是否為可信賴的。

28. 如申請專利範圍第26項之機器可讀取之媒體，其中該訊息包含用來確認該用戶端裝置的身分之一用戶端裝置憑證，且該執行適當的身分鑑定包含下列步驟：確認該用戶端裝置憑證。

29. 如申請專利範圍第26項之機器可讀取之媒體，其中該等身分鑑定功能包含下列步驟：

該安全系統代表該伺服器而向該用戶端裝置要求身分鑑定；

自該用戶端裝置接收一用戶端裝置憑證；以及

決定該用戶端裝置是否為可信賴的，且係由代表該

伺服器的該安全系統上執行該決定步驟。

30. 一種裝置，包含：

至少一個處理器；以及

一機器可讀取之媒體，該機器可讀取之媒體中具有編碼的指令，而當該處理器執行該等編碼的指令時，該等編碼的指令可指示該處理器執行下列步驟：

接收自一用戶端裝置傳送到一伺服器之訊息，該訊息係用來建立一安全連線；

在與該伺服器相關聯的一安全系統上擷截該資料，以便執行各身分鑑定功能；以及

如果執行了適當的身分鑑定，則建立一安全連線。

31. 如申請專利範圍第30項之裝置，其中該適當的身分鑑定包含下列步驟：如果該用戶端裝置已要求身分鑑定，則決定該伺服器是否為可信賴的。

32. 如申請專利範圍第30項之裝置，其中該訊息包含用來確認該用戶端裝置的身分之一用戶端裝置憑證，且該執行適當的身分鑑定包含下列步驟：確認該用戶端裝置憑證。

FREE

拾壹、圖式

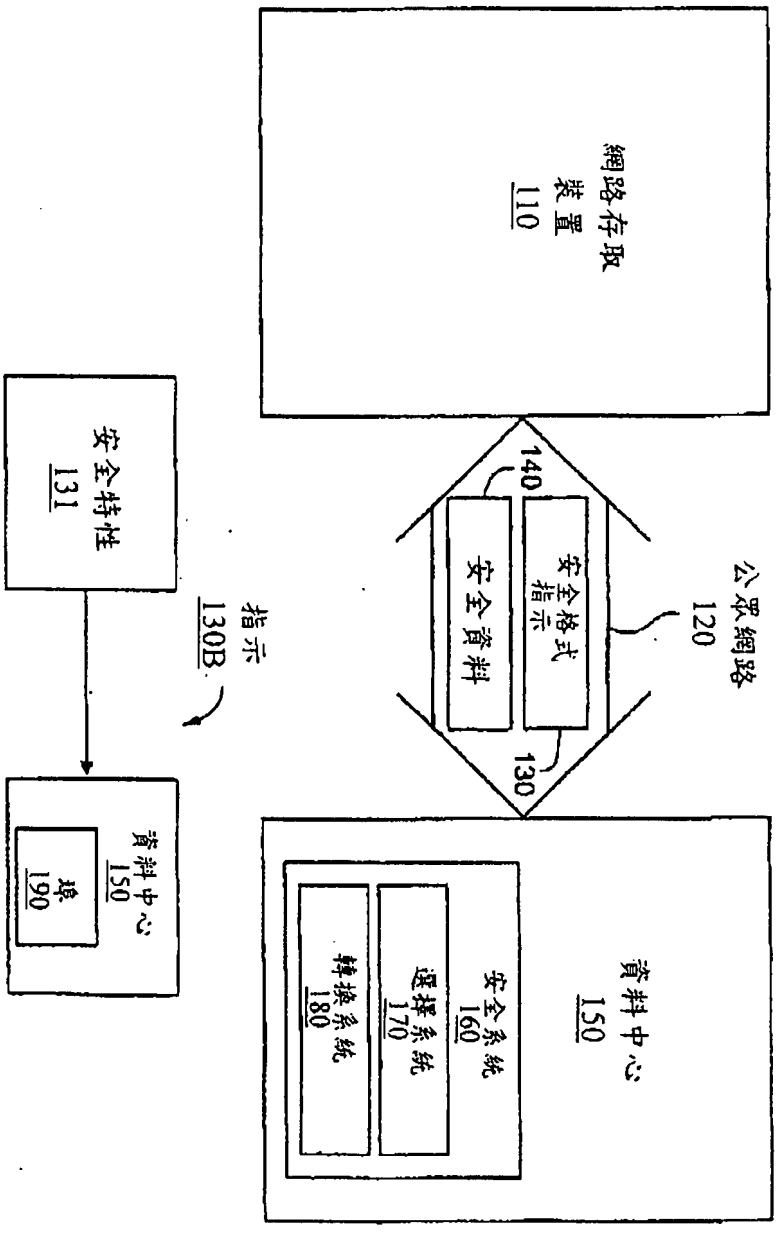
100
網路存取裝置 110
公眾網路 120
140
安全格式指示
安全資料
130
資料中心 150
安全系統 160
選擇系統 170
轉換系統 180
指示 130B
安全特性 131
資料中心 150
埠 190

圖 1

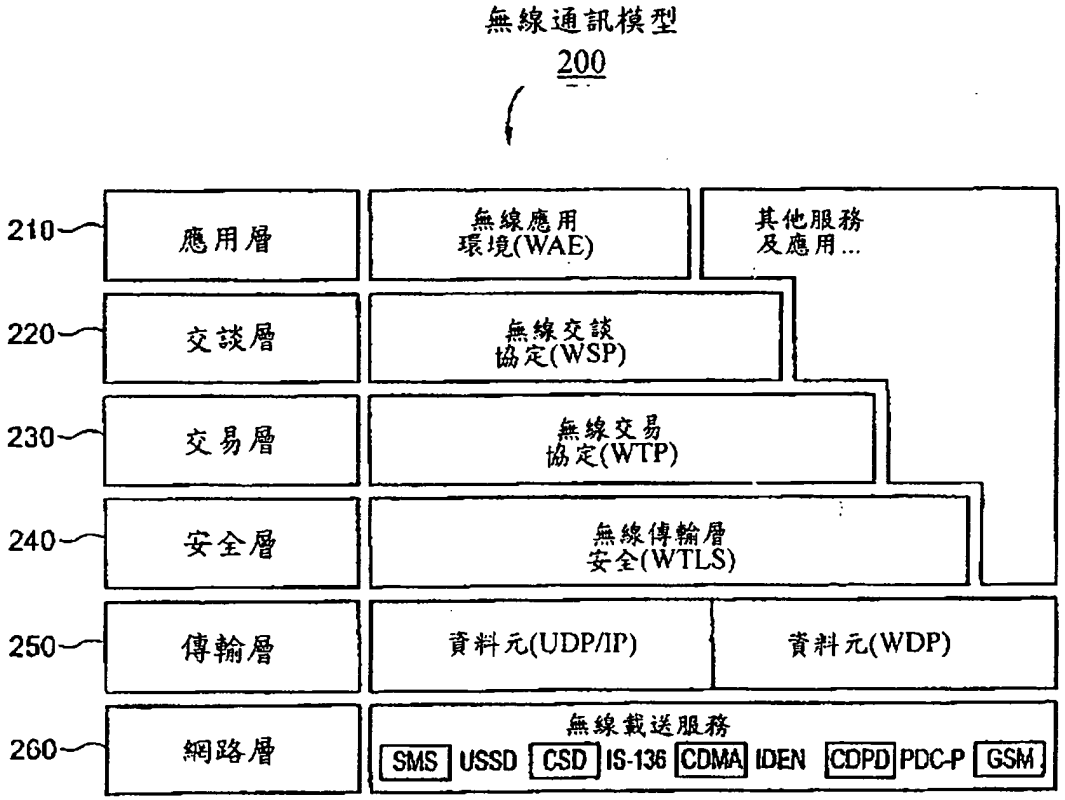

圖 2

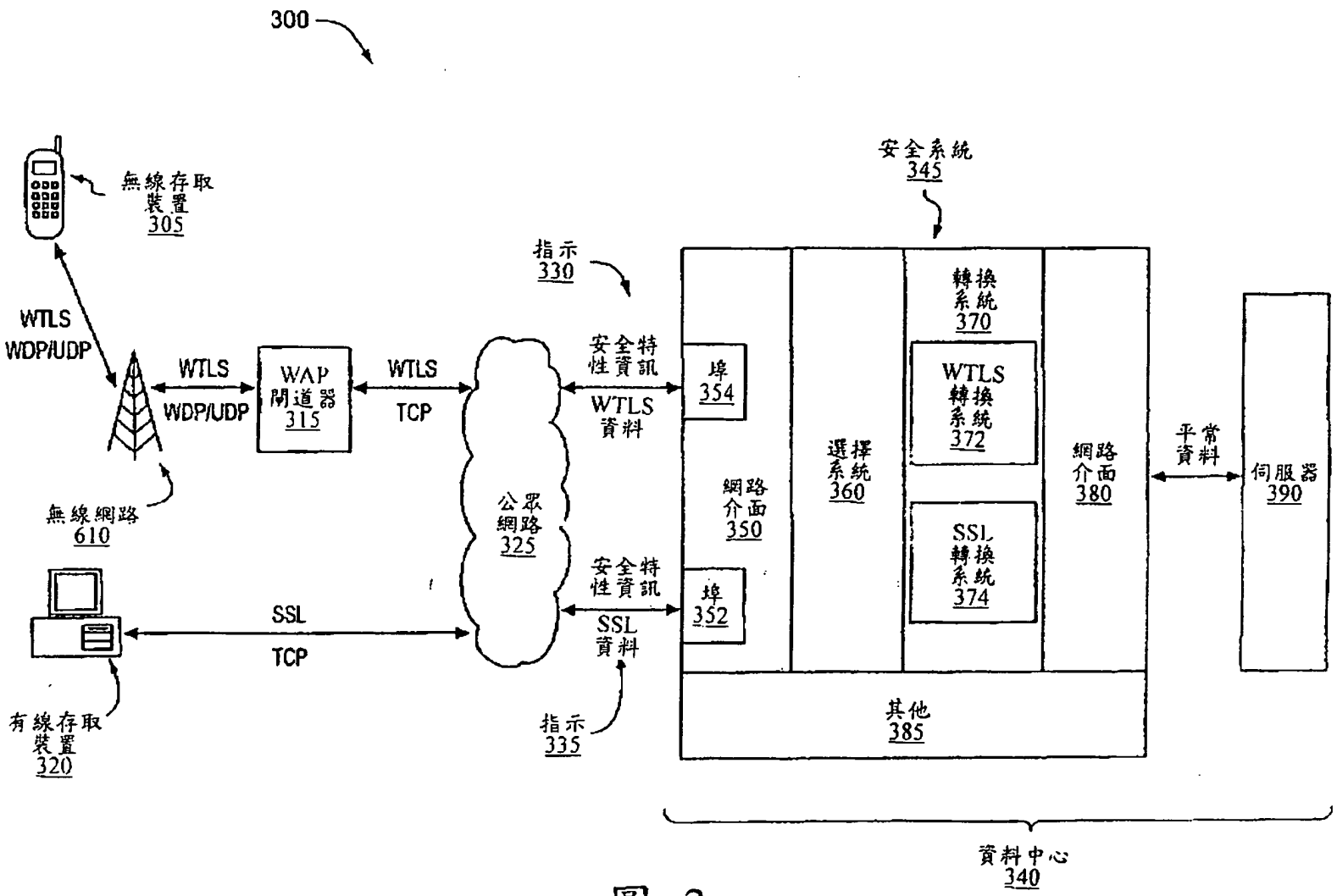
300
無線存取裝置 305
WTLS
WDP/UDP
WTLS
WDP/UDP
WAP 閘道器 315
WTLS
TCP
無線網路 610
公眾網路 325
SSL
TCP
有線存取裝置 320
指示 330
安全特性資訊
WTLS 資料
安全特性資訊
SSL 資料
指示 335
安全系統 345
埠 354
埠 352
網路介面 350
選擇系統 360
轉換系統 370
WTLS 轉換系統 372
SSL 轉換系統 374
網路介面 380
其他 385
平常資料
伺服器 390
資料中心 340

圖 3

圖式續頁

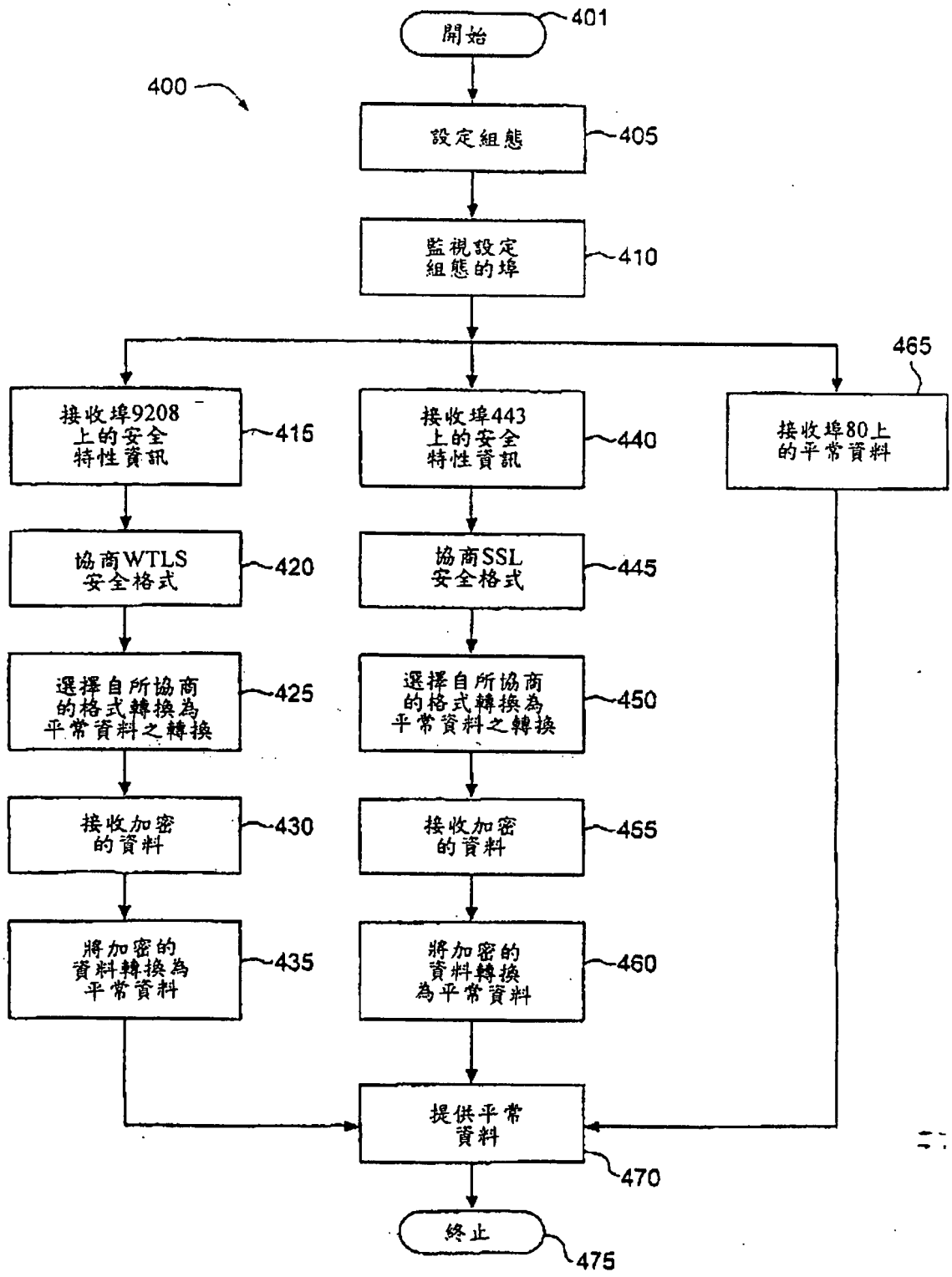
400
開始
401
設定組態
405
監視設定組態的埠
410
465
接收埠9208上的安全特性資訊
415
協商WTLS安全格式
420
選擇自所協商的格式轉換為平常資料之轉換
425
接收加密的資料
430
將加密的資料轉換為平常資料
435
接收埠443上的安全特性資訊
440
協商SSL安全格式
445
選擇自所協商的格式轉換為平常資料之轉換
450
接收加密的資料
455
將加密的資料轉換為平常資料
460
接收埠80上的平常資料
提供平常資料
470
終止
475

圖 4

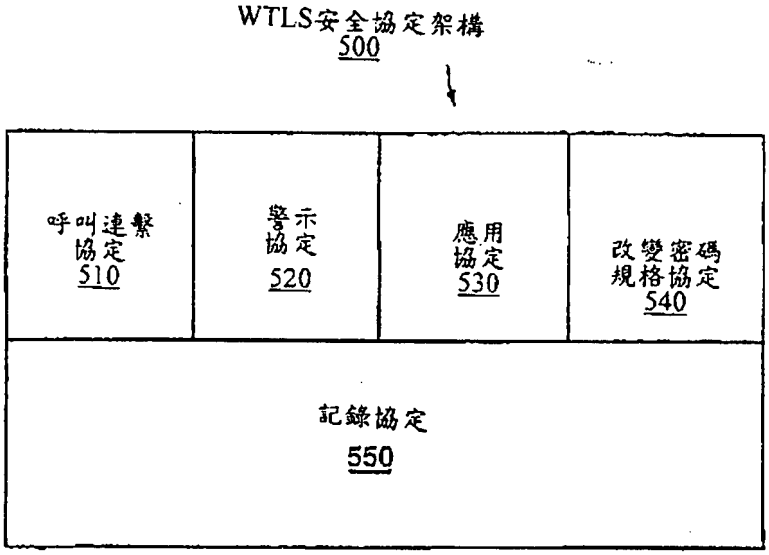

圖 5

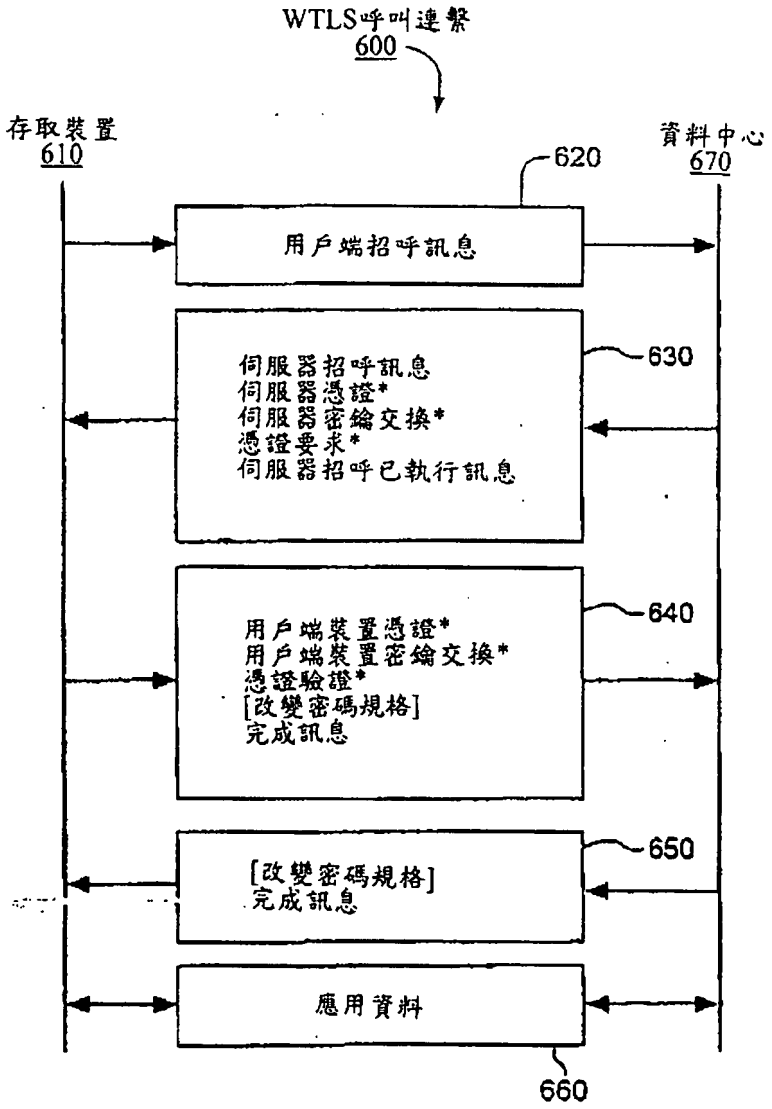
WTLS呼叫連繫
600
存取裝置
610
資料中心
670
620
用戶端招呼訊息
伺服器招呼訊息
伺服器憑證*
伺服器密鑰交換*
憑證要求*
伺服器招呼已執行訊息
630
用戶端裝置憑證*
用戶端裝置密鑰交換*
憑證驗證*
[改變密碼規格]
完成訊息
640
[改變密碼規格]
完成訊息
650
應用資料
660

圖 6

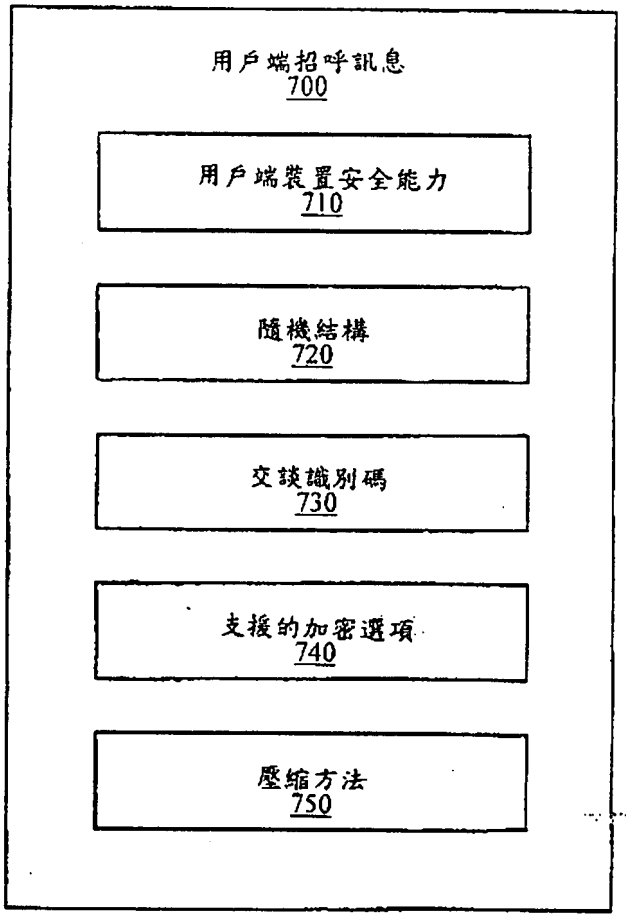

圖 7

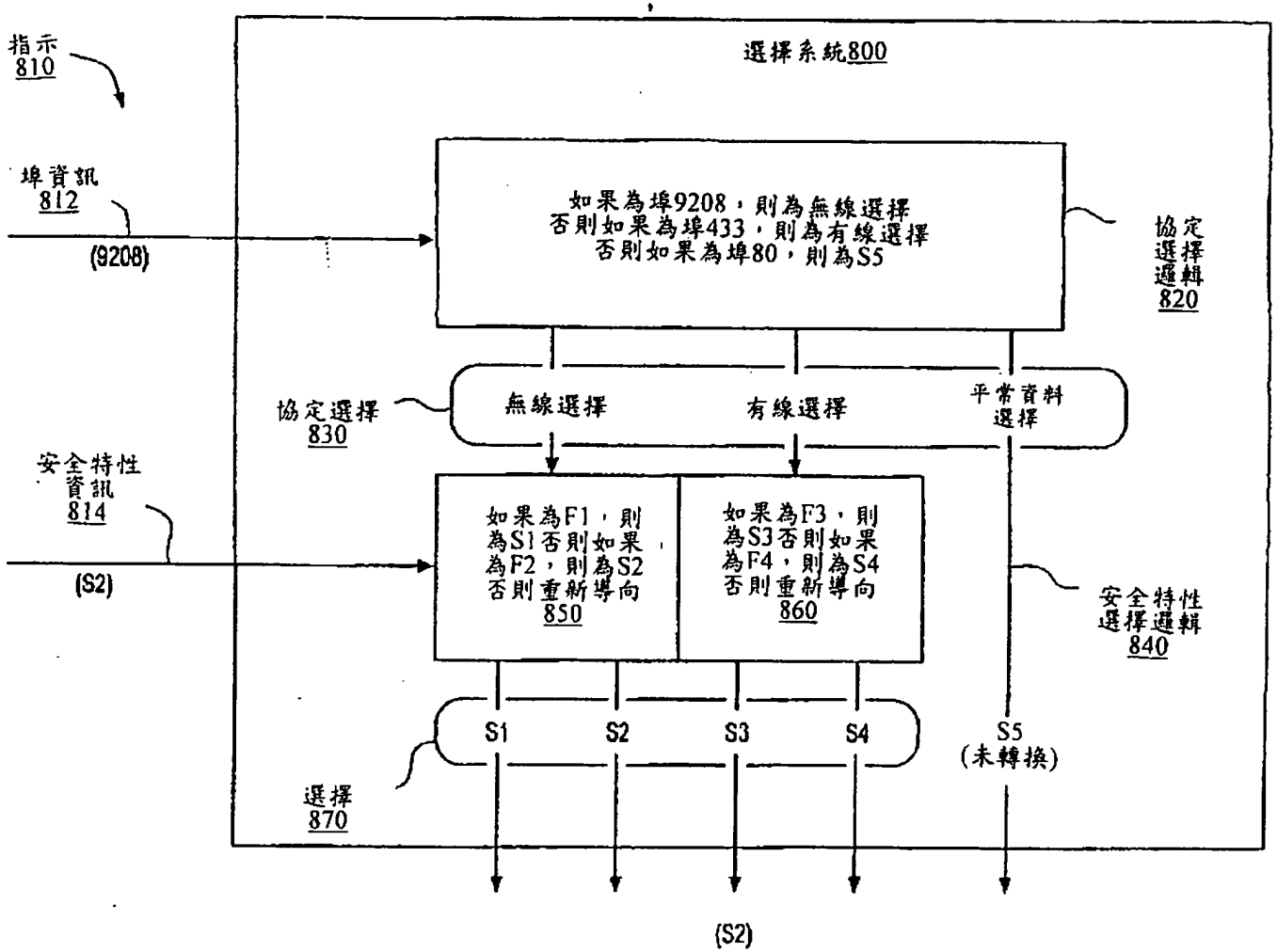
選擇系統800
指示
810
埠資訊
812
(9208)
如果為埠9208，則為無線選擇
否則如果為埠433，則為有線選擇
否則如果為埠80，則為S5
協定
選擇
邏輯
820
協定選擇
830
無線選擇
有線選擇
平常資料
選擇
安全特性
資訊
814
(S2)
如果為F1，則
為S1否則如果
為F2，則為S2
否則重新導向
850
如果為F3，則
為S3否則如果
為F4，則為S4
否則重新導向
860
安全特性
選擇邏輯
840
S1
S2
S3
S4
S5
(未轉換)
選擇
870
(S2)

圖 8

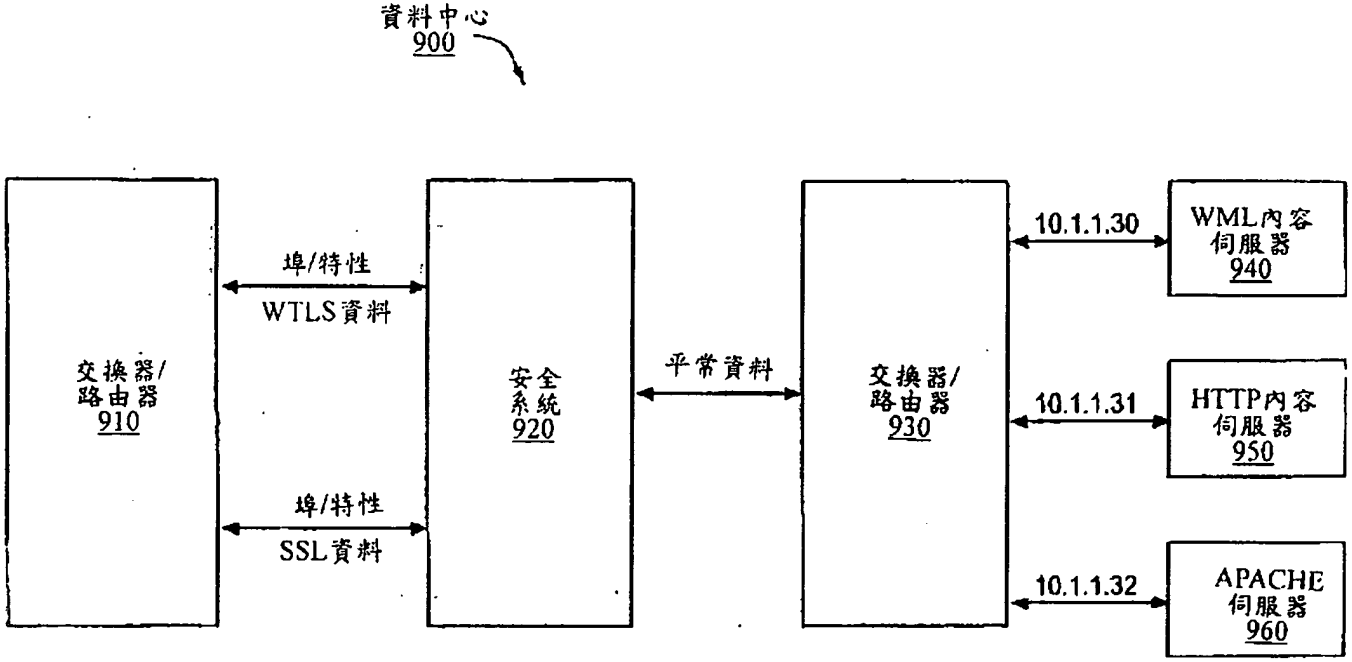

圖 9

圖式續頁

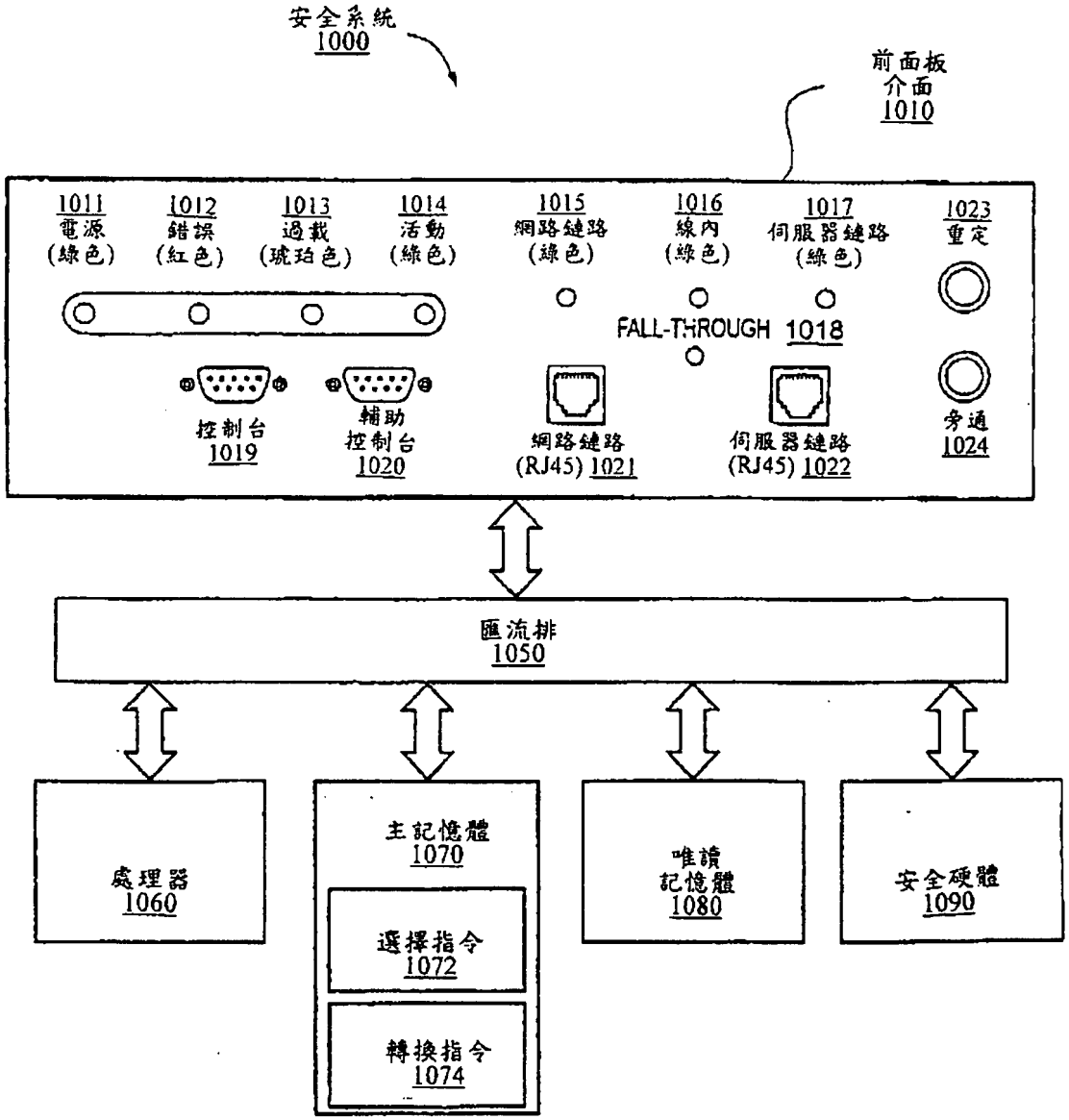

圖 10

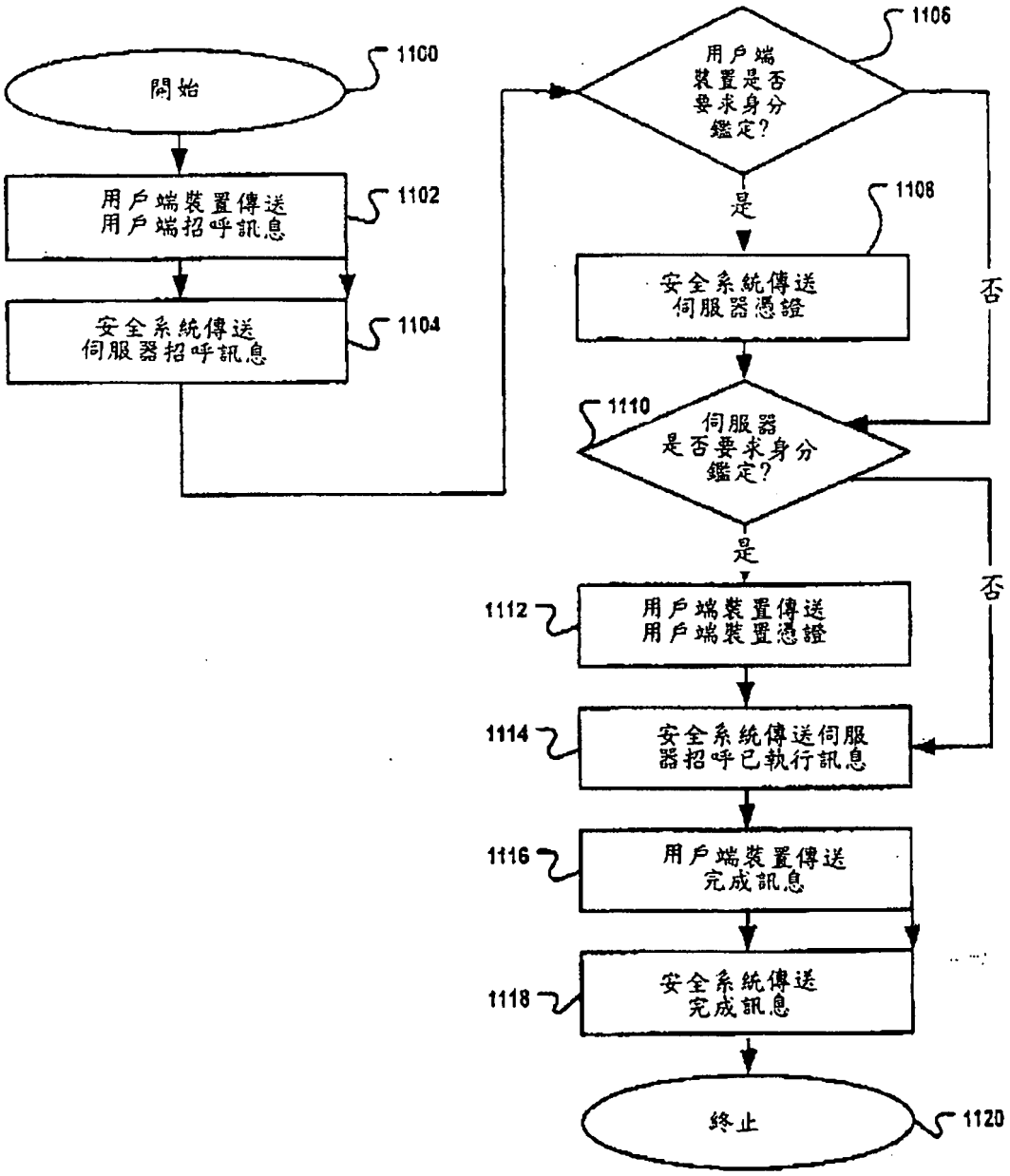
開始
1100
用戶端裝置傳送
用戶端招呼訊息
1102
安全系統傳送
伺服器招呼訊息
1104
用戶端
裝置是否
要求身分
鑑定?
1106
是
否
安全系統傳送
伺服器憑證
1108
伺服器
是否要求身分
鑑定?
1110
是
否
用戶端裝置傳送
用戶端裝置憑證
1112
安全系統傳送伺服
器招呼已執行訊息
1114
用戶端裝置傳送
完成訊息
1116
安全系統傳送
完成訊息
1118
終止
1120

圖 11

圖式續頁

```
1   BEGIN
2
3   DETECT METHOD OF ENCRYPTION
4        SWITCH DATA_TYPE
5             CASE: WTLS
6                  START WTLS HANDSHAKE
7                  COMPLETE AUTHENTICATION
8                  DECRYPT WTLS
9             CASE: SSL
10                 START SSL HANDSHAKE
11                 COMPLETE AUTHENTICATION
12                 DECRYPT SSL
13            CASE: PLAIN
14                 DO NOTHING
15  END
```

圖 12

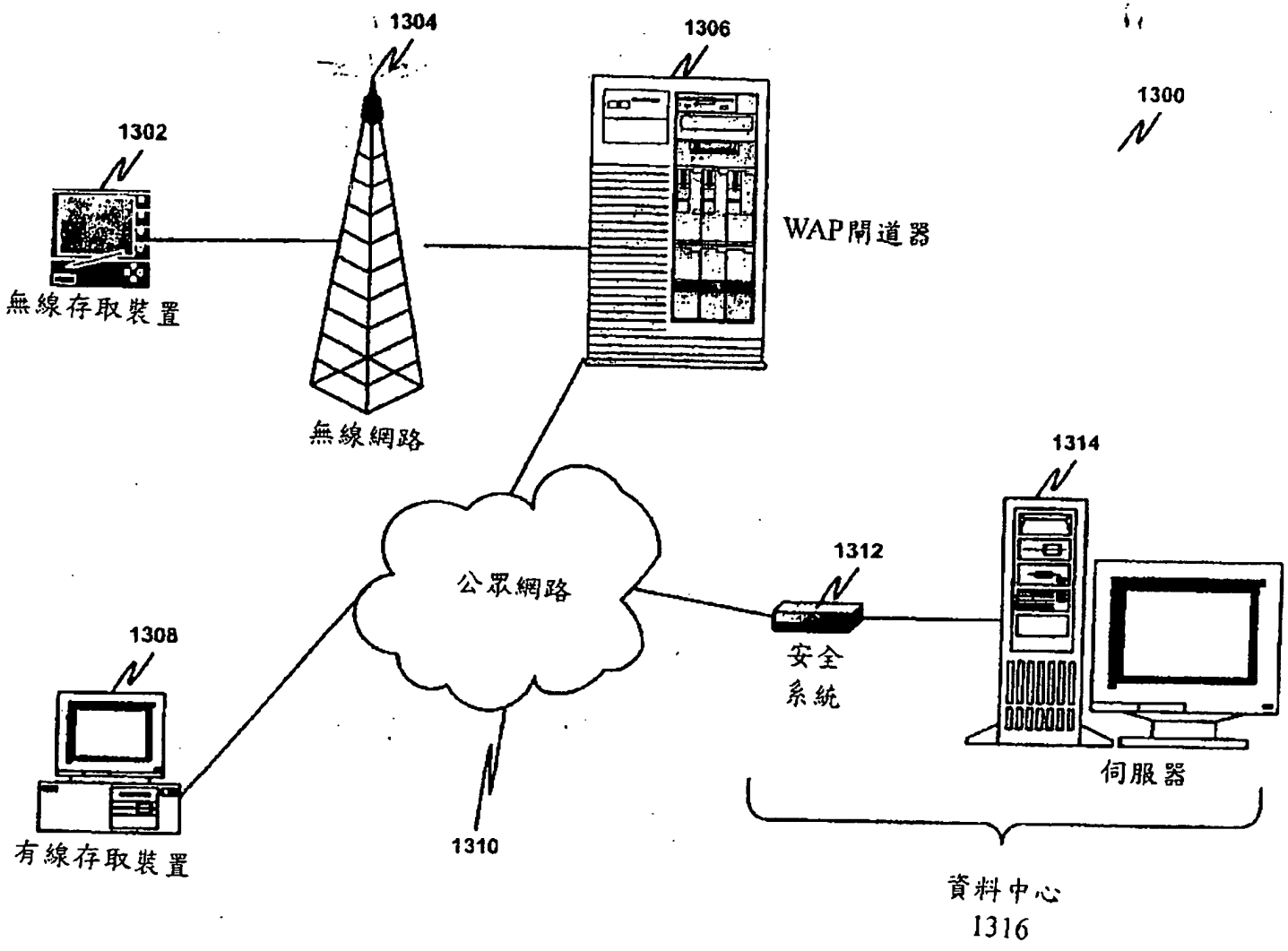

圖 13

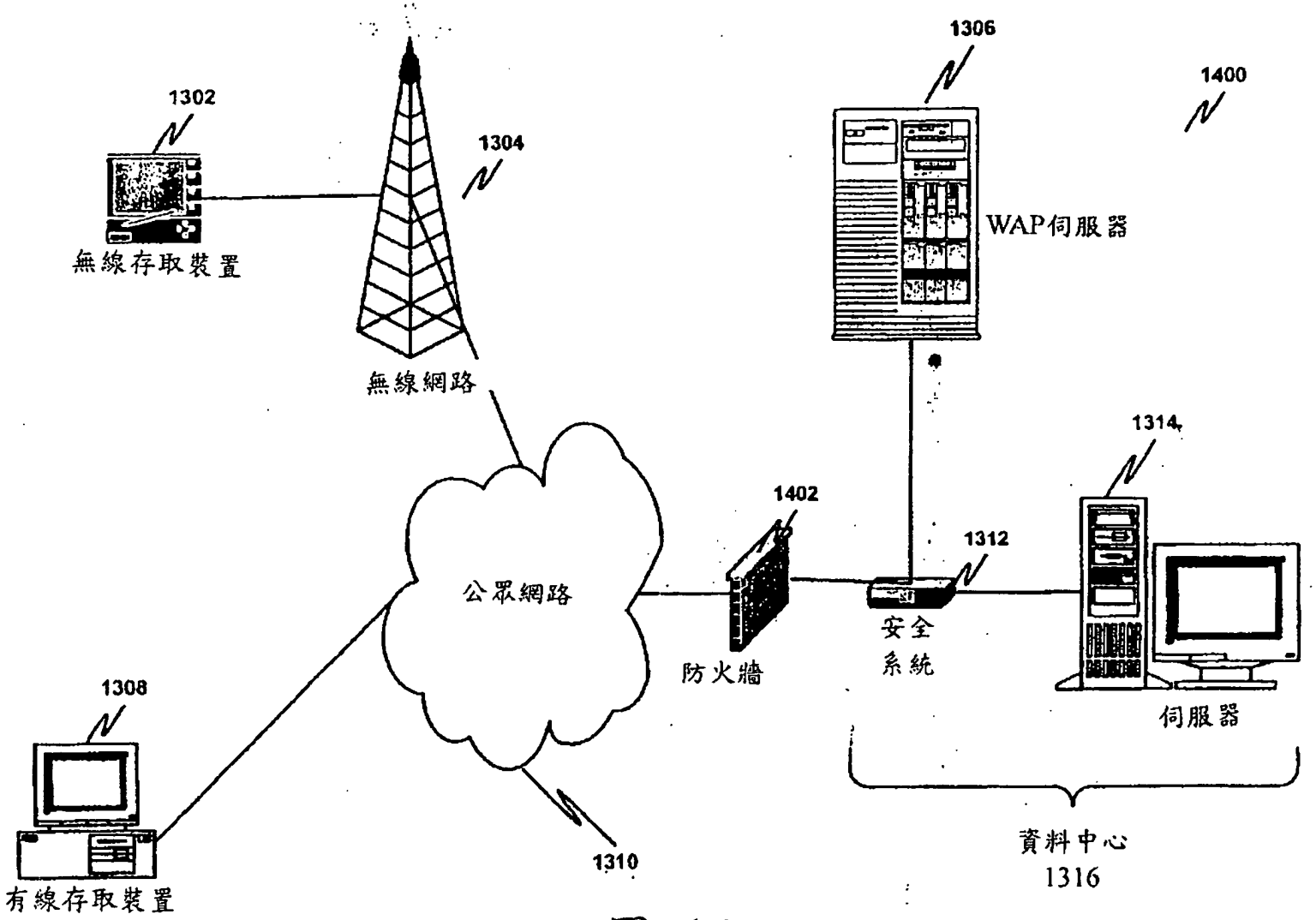
1302
無線存取裝置
1304
無線網路
1306
WAP伺服器
1400
1314
1402
1312
公眾網路
防火牆
安全
系統
伺服器
1308
1310
有線存取裝置
資料中心
1316

圖 14

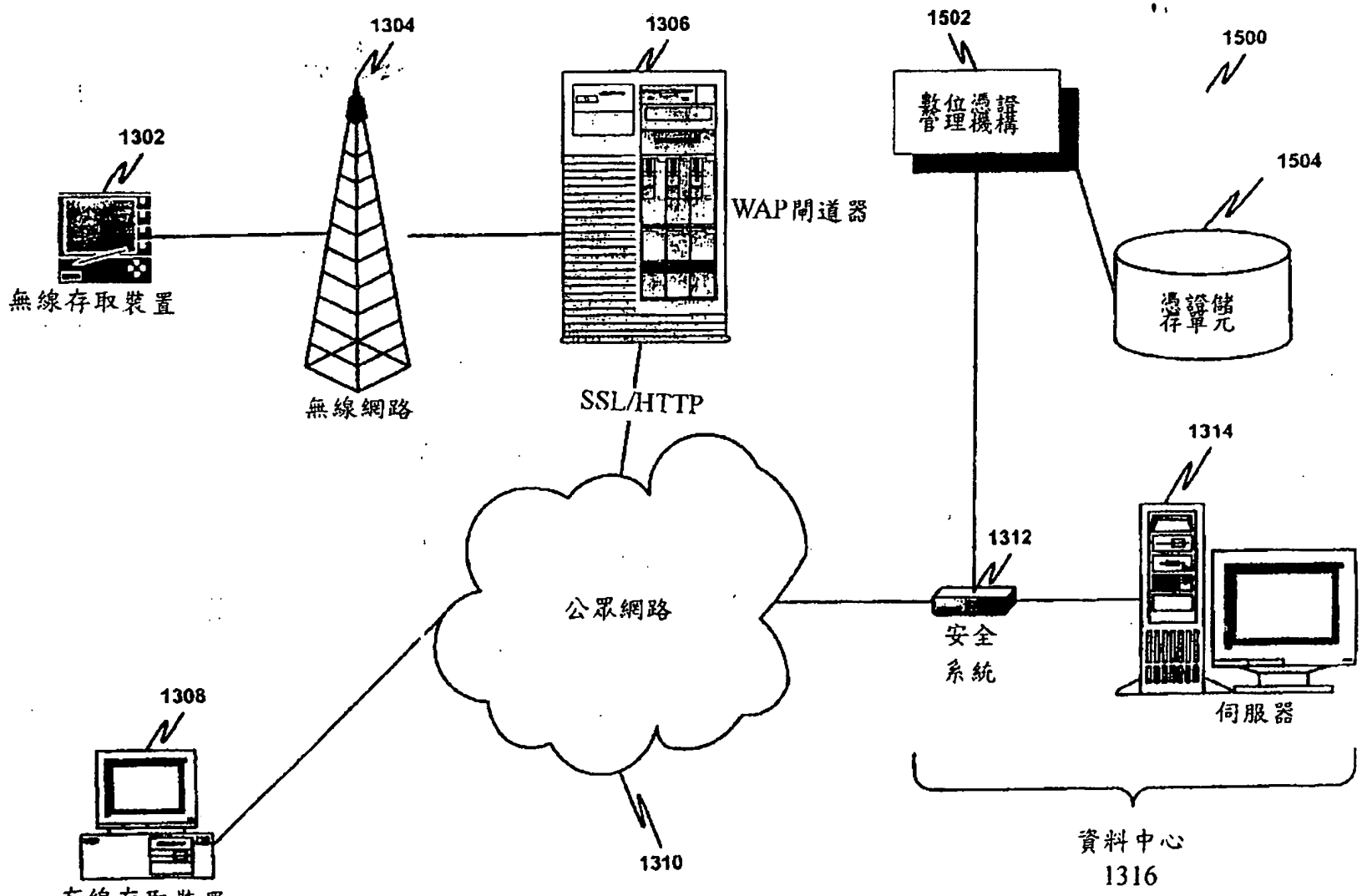
1304
1306
1502
1500
1302
WAP閘道器
數位憑證管理機構
1504
憑證儲存單元
無線存取裝置
無線網路
SSL/HTTP
1314
1312
公眾網路
安全系統
伺服器
1308
1310
資料中心
1316
有線存取裝置

圖 15

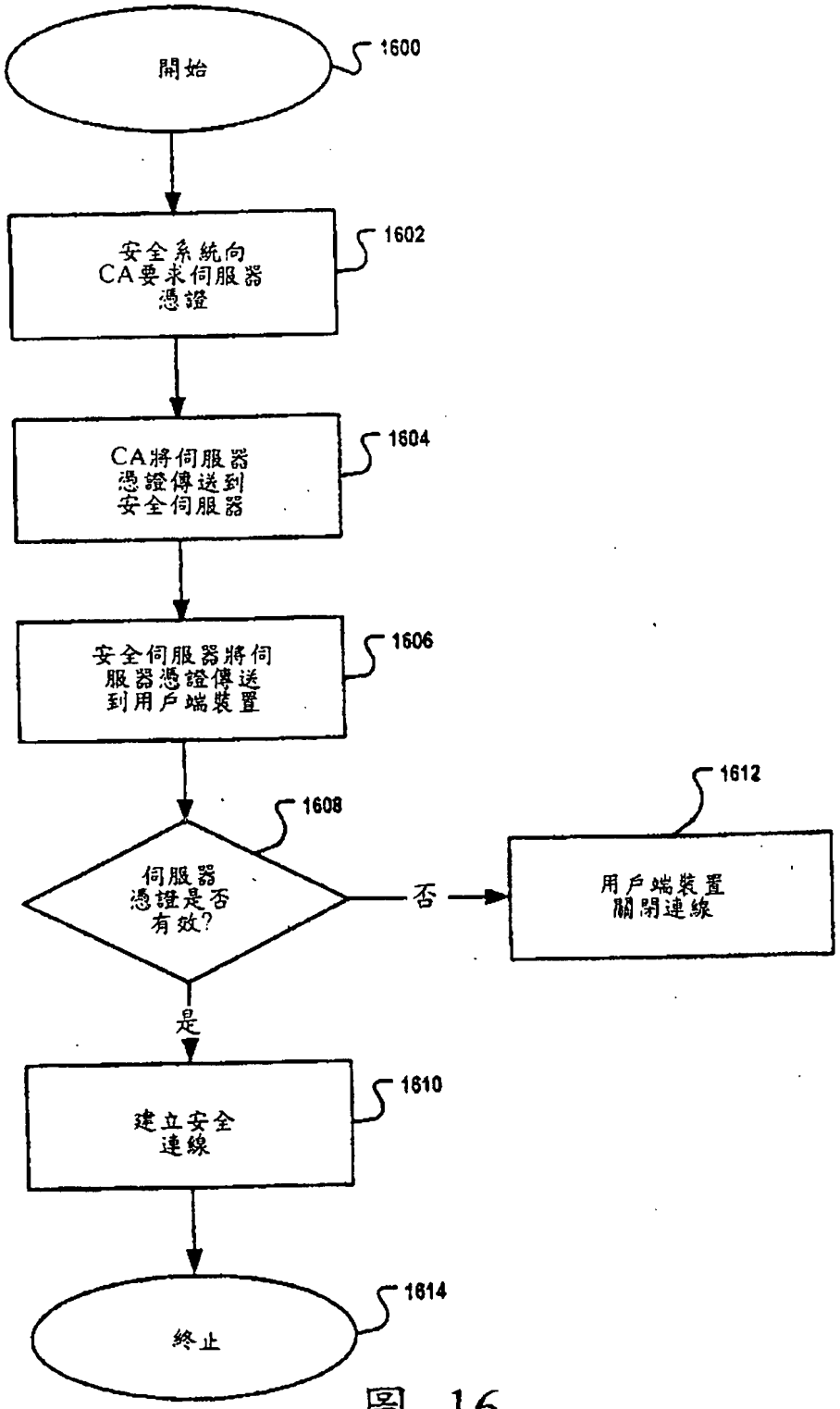
開始
1600
安全系統向CA要求伺服器憑證
1602
CA將伺服器憑證傳送到安全伺服器
1604
安全伺服器將伺服器憑證傳送到用戶端裝置
1606
伺服器憑證是否有效?
1608
否
用戶端裝置關閉連線
1612
是
建立安全連線
1610
終止
1614

圖 16

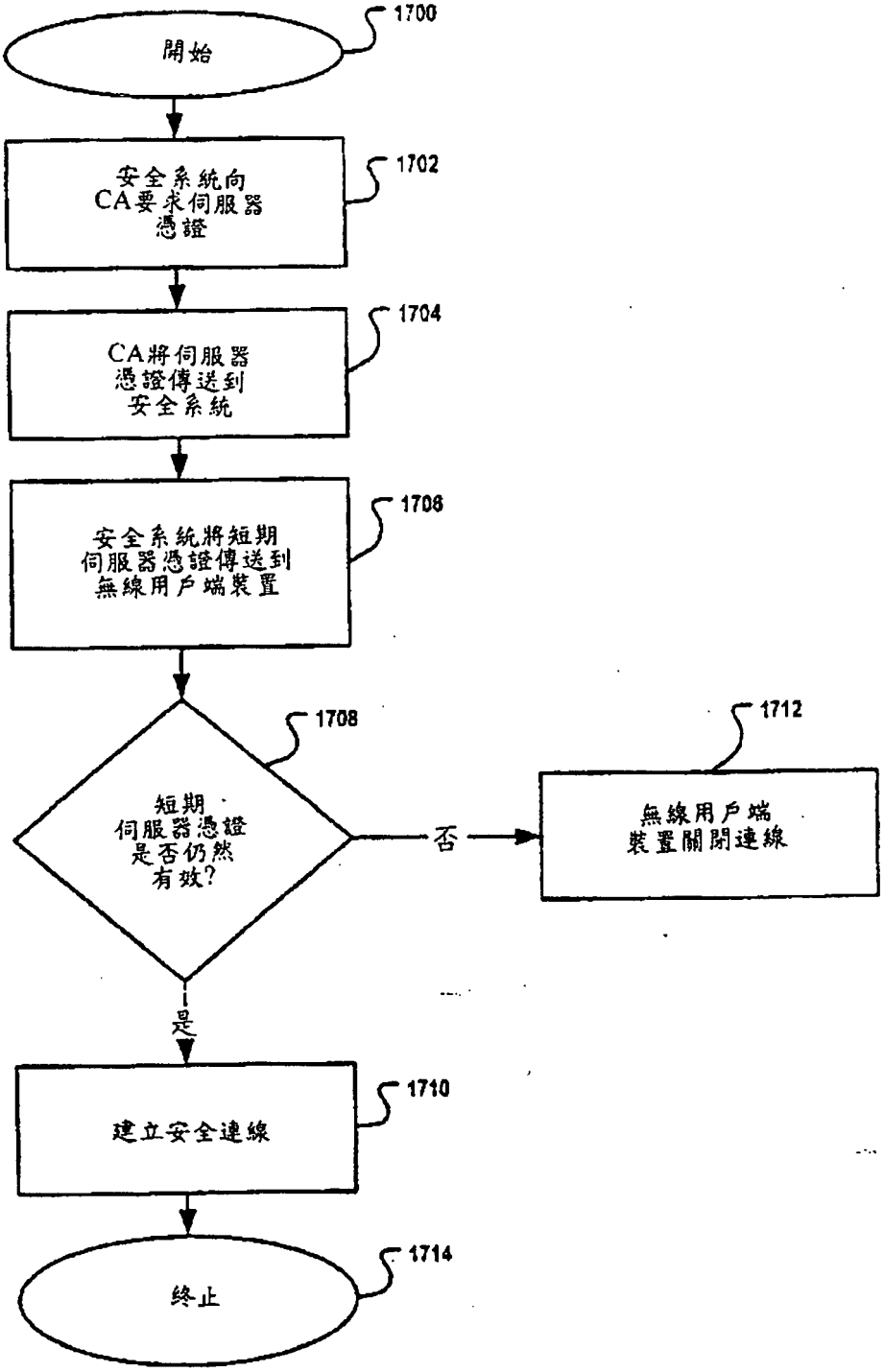
1700
開始
安全系統向CA要求伺服器憑證
1702
CA將伺服器憑證傳送到安全系統
1704
安全系統將短期伺服器憑證傳送到無線用戶端裝置
1706
短期伺服器憑證是否仍然有效?
1708
否
無線用戶端裝置關閉連線
1712
是
建立安全連線
1710
終止
1714

圖 17

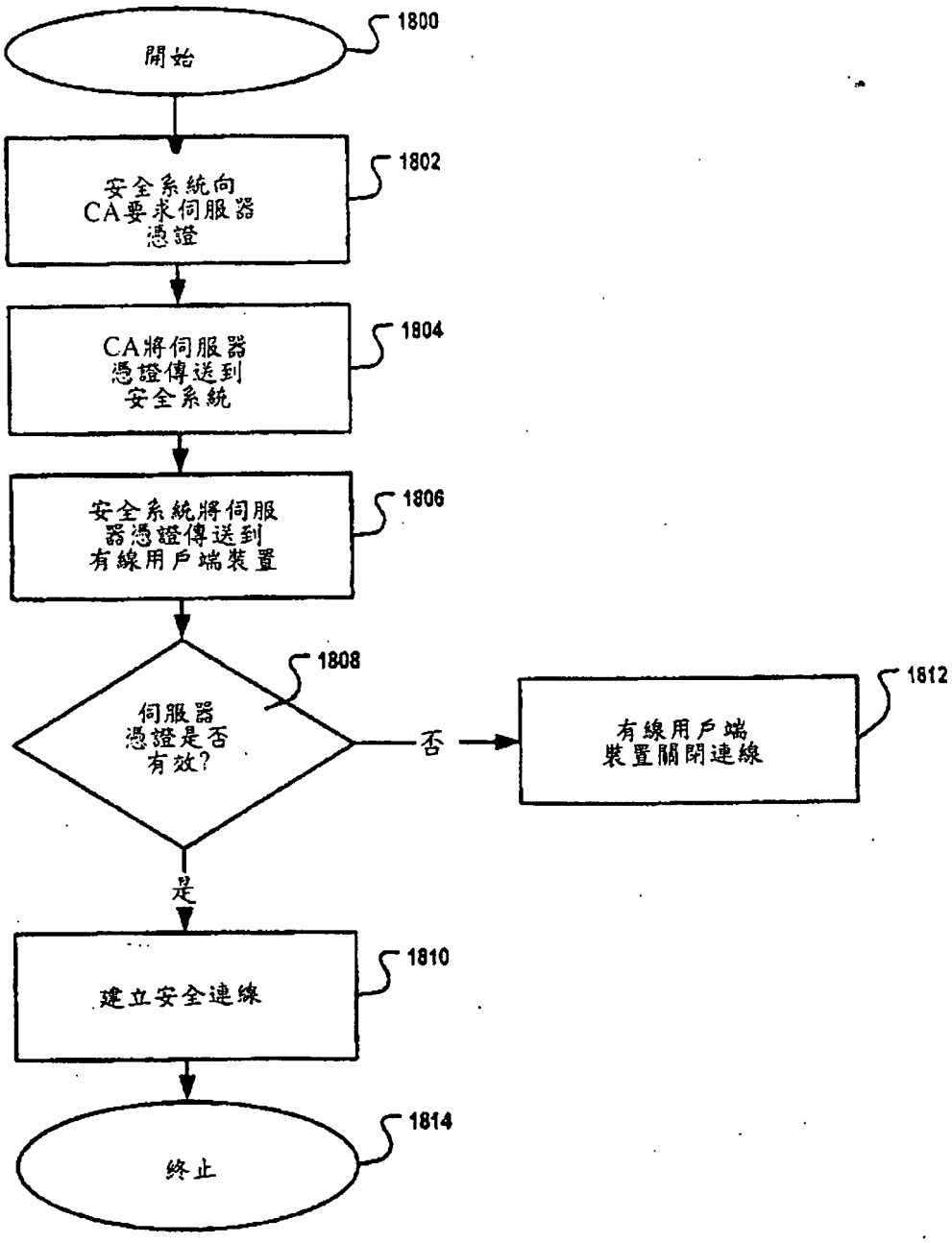

圖 18

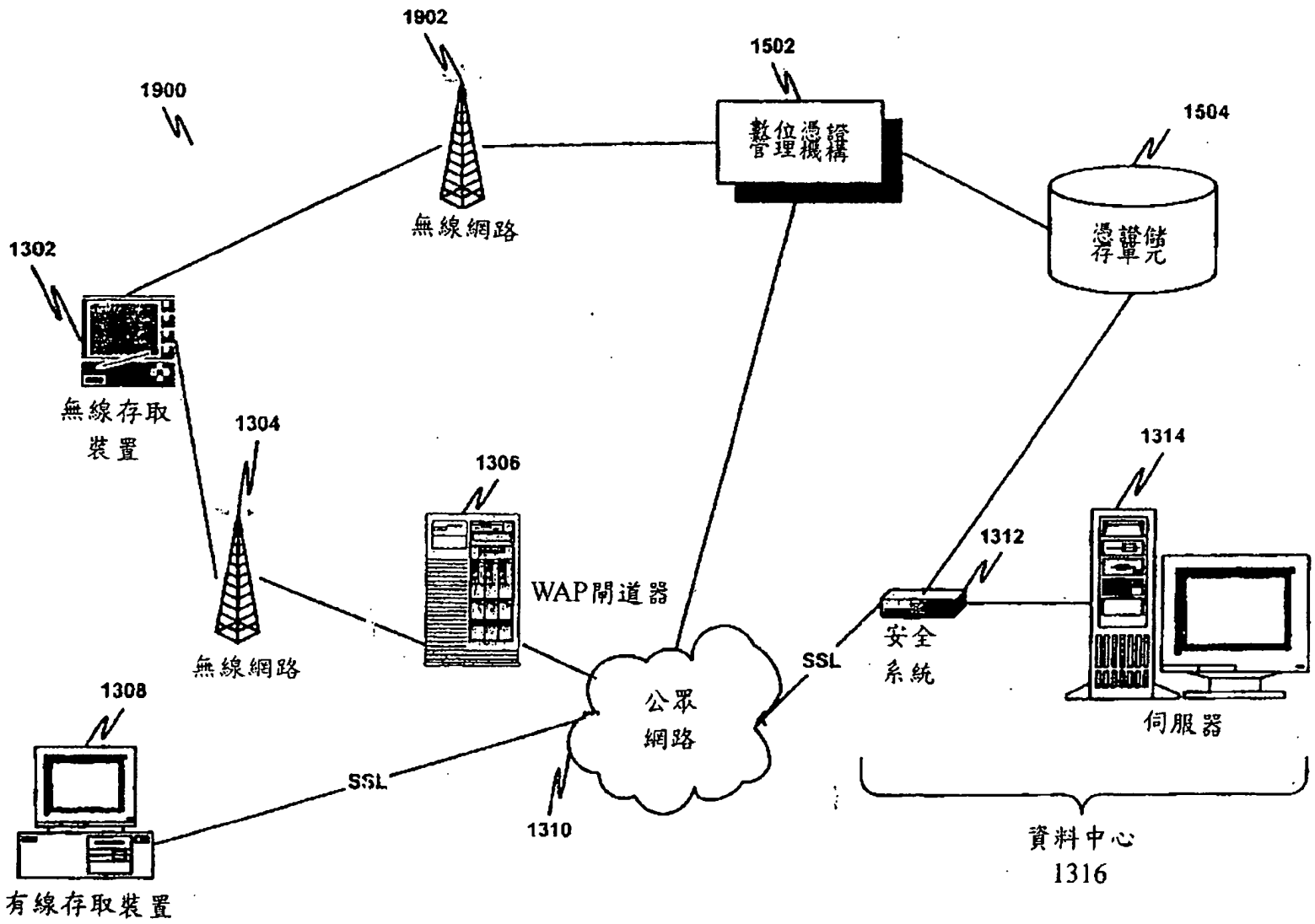
1900
1902
無線網路
1502
數位憑證管理機構
1504
憑證儲存單元
1302
無線存取裝置
1304
無線網路
1306
WAP閘道器
1308
有線存取裝置
SSL
1310
公眾網路
SSL
1312
安全系統
1314
伺服器
資料中心
1316

圖 19

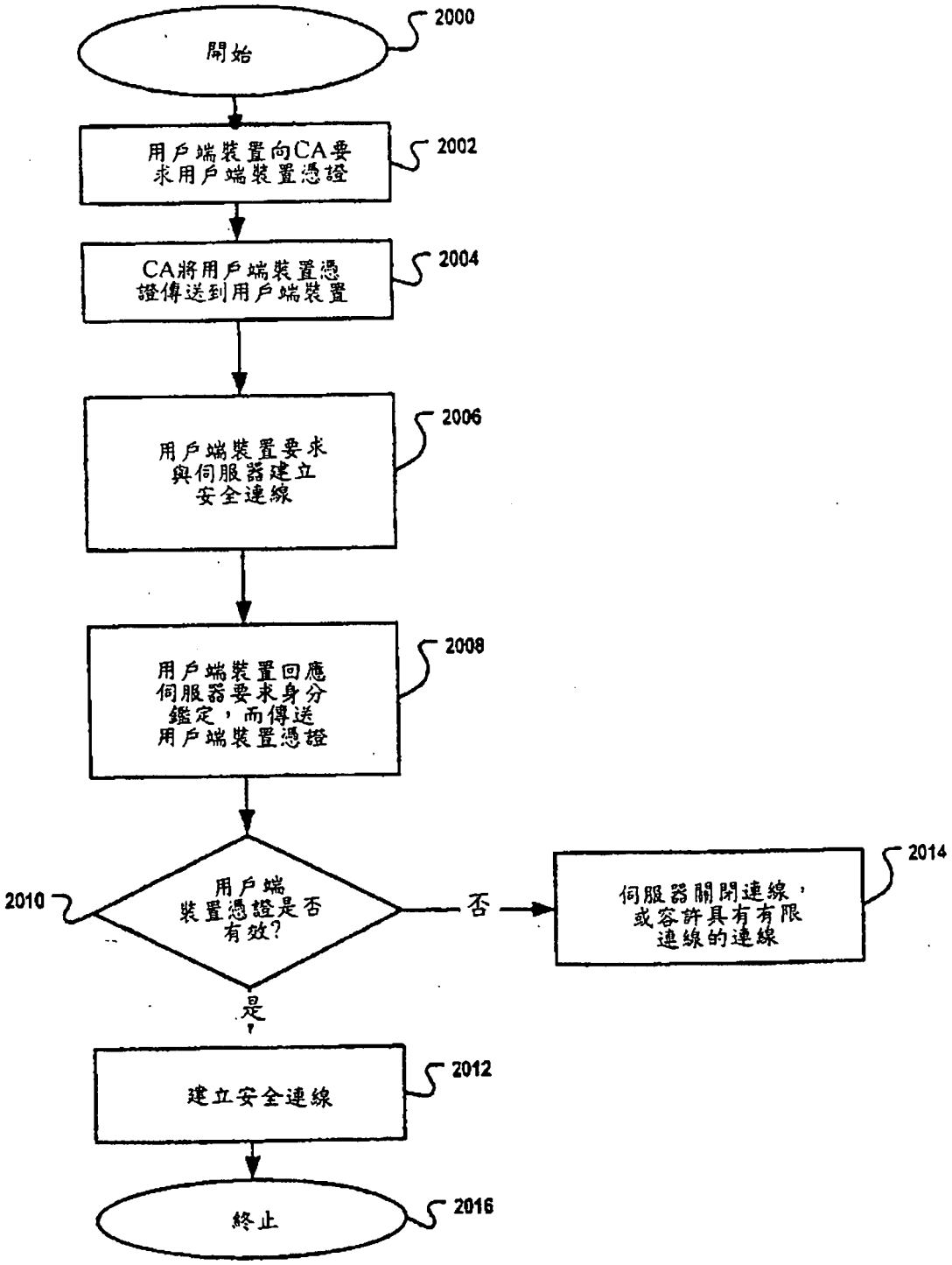
開始
2000
用戶端裝置向CA要求用戶端裝置憑證
2002
CA將用戶端裝置憑證傳送到用戶端裝置
2004
用戶端裝置要求與伺服器建立安全連線
2006
用戶端裝置回應伺服器要求身分鑑定，而傳送用戶端裝置憑證
2008
用戶端裝置憑證是否有效?
2010
否
伺服器關閉連線，或容許具有有限連線的連線
2014
是
建立安全連線
2012
終止
2016

圖 20

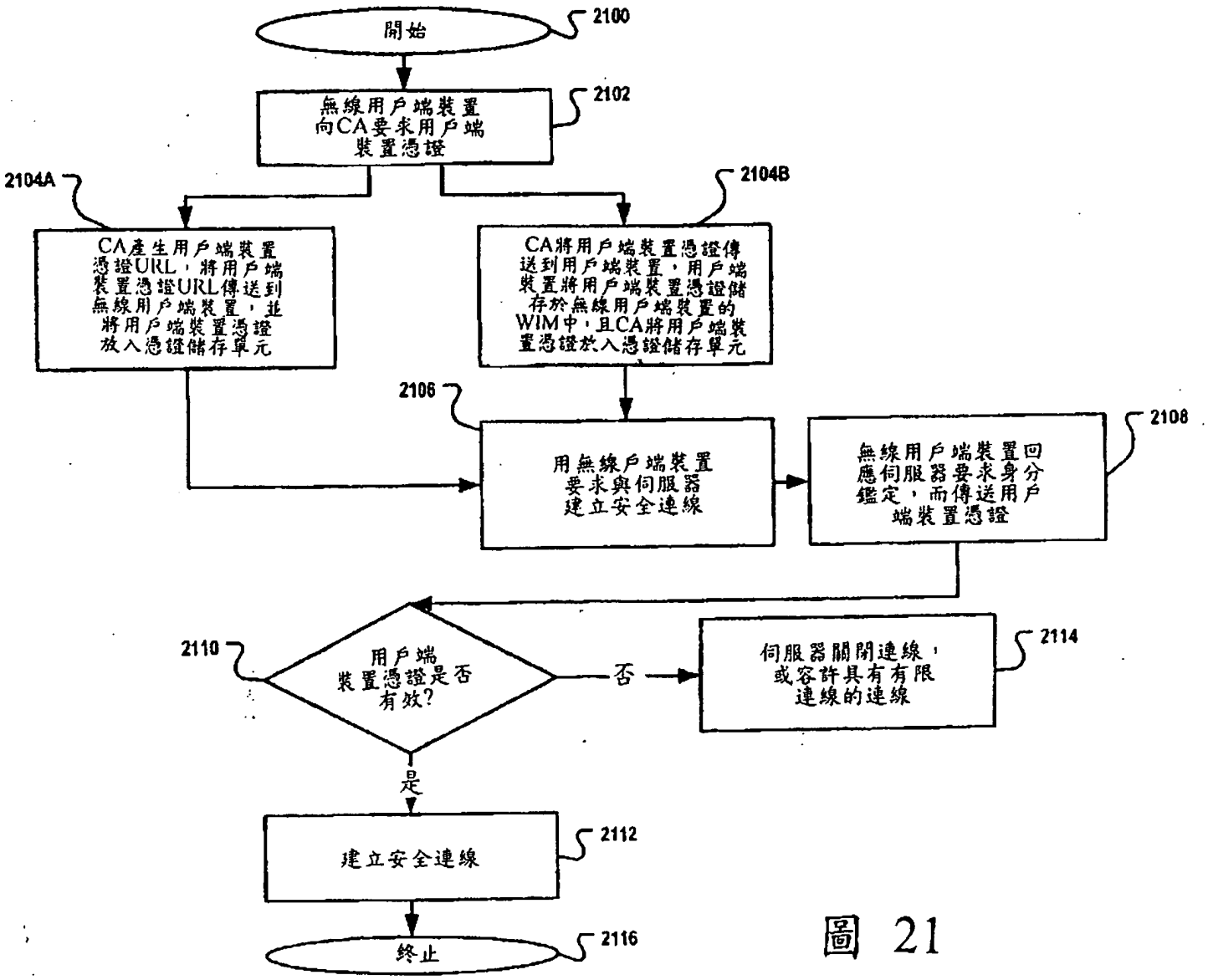
開始
2100
無線用戶端裝置向CA要求用戶端裝置憑證
2102
2104A
CA產生用戶端裝置憑證URL，將用戶端裝置憑證URL傳送到無線用戶端裝置，並將用戶端裝置憑證放入憑證儲存單元
2104B
CA將用戶端裝置憑證傳送到用戶端裝置，用戶端裝置將用戶端裝置憑證儲存於無線用戶端裝置的WIM中，且CA將用戶端裝置憑證放入憑證儲存單元
2106
用無線戶端裝置要求與伺服器建立安全連線
無線用戶端裝置回應伺服器要求身分鑑定，而傳送用戶端裝置憑證
2108
2110
用戶端裝置憑證是否有效?
否
伺服器關閉連線，或容許具有有限連線的連線
2114
是
建立安全連線
2112
終止
2116

圖 21

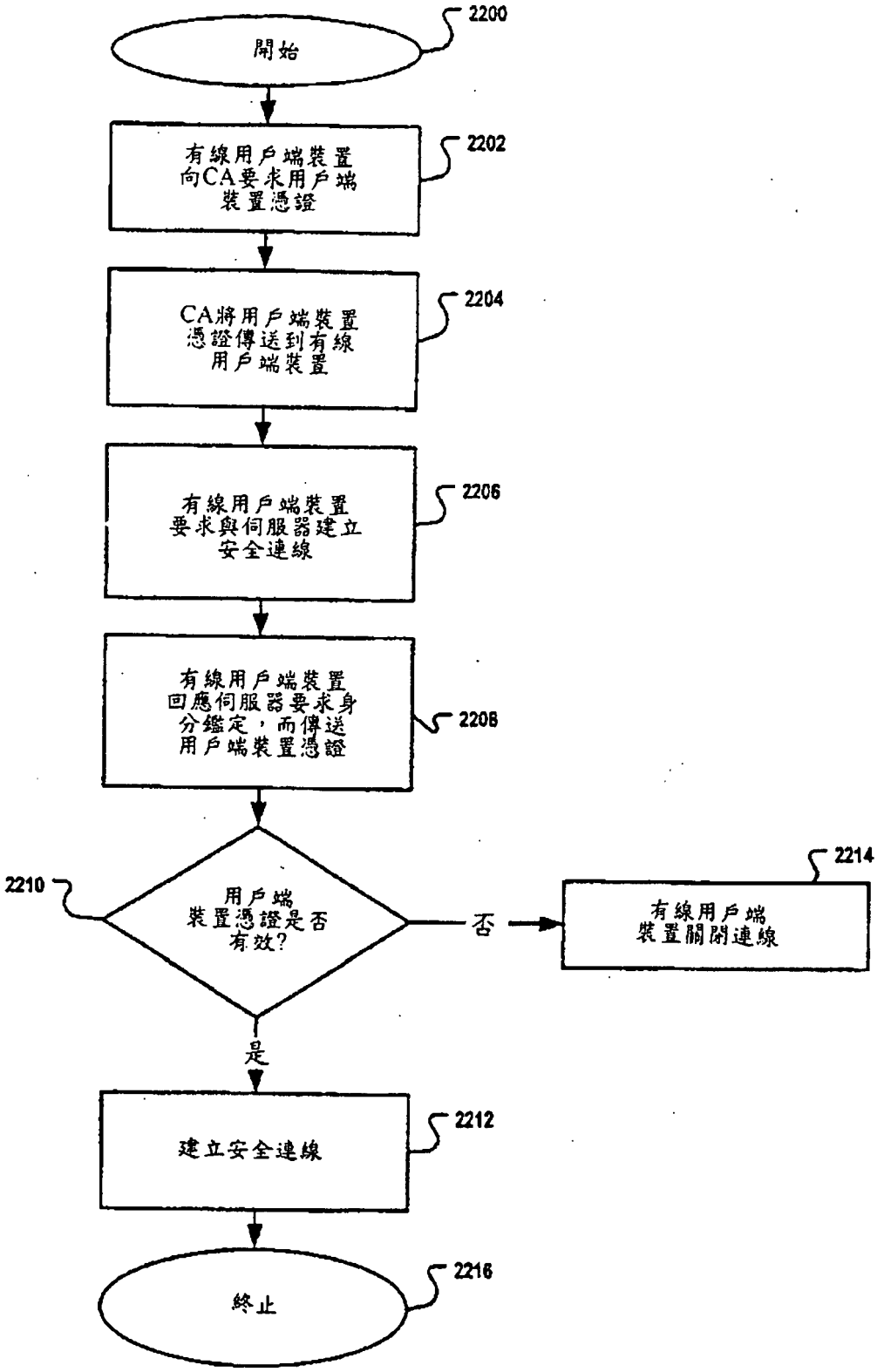

圖 22

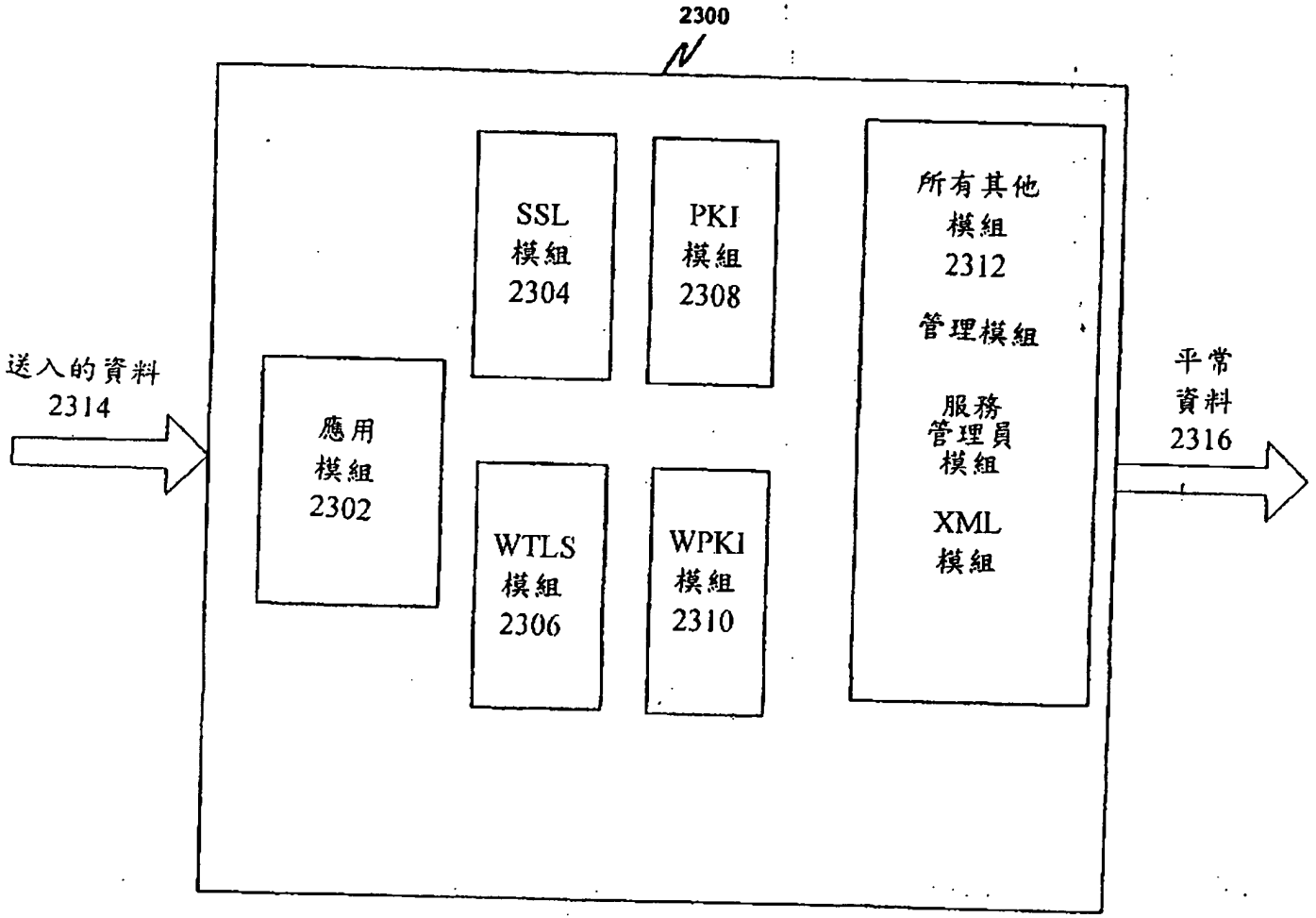
2300
送入的資料
2314
應用
模組
2302
SSL
模組
2304
PKI
模組
2308
WTLS
模組
2306
WPKI
模組
2310
所有其他
模組
2312
管理模組
服務
管理員
模組
XML
模組
平常
資料
2316

圖 23

連線圖識別碼	連線類型	密鑰識別碼	伺服器IP	網路埠	伺服器埠	密碼套件	重新導向	用戶端身分鑑定	數位簽章
1	WTLS	mysrv1	10.1.1.30	9202	80	低	n	y	y
2	SSL	mysrv2	10.1.1.30	443	80	中等(v2+v3)	n	y	y
3	平常資料	無	10.1.1.30	8080	80	無	n	n	n

圖 24